

## Safety Manager Safety Manual

EP-SM.MAN.6283

100.3

25 January 2005

**Release 100.3**

# Honeywell

Document	Release	Date
EP-SM.MAN.6283	100.3	January 2005

## Notice

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell Safety Management Systems.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Copyright 2004 – Honeywell Safety Management Systems, a division of Honeywell Aerospace B.V.

## Honeywell trademarks

Safety Manager™ is a trademark of Honeywell International Inc.

Experion PKS®, PlantScape®, SafeBrowse®, TotalPlant® and TDC 3000® are U.S. registered trademarks of Honeywell International Inc.

## Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

## Support and other contacts

### United States and Canada

**Contact:** Honeywell IAC Solution Support Center  
**Phone:** 1-800 822-7673. In Arizona: (602) 313-5558  
Calls are answered by dispatcher between 6:00 am and 4:00 pm Mountain Standard Time. Emergency calls outside normal working hours are received by an answering service and returned within one hour.  
**Facsimile:** (602) 313-5476  
**Mail:** Honeywell IS TAC, MS P13  
2500 West Union Hills Drive  
Phoenix, AZ, 85027

### Europe

**Contact:** Honeywell PACE TAC  
**Phone:** +32-2-728-2657  
**Facsimile:** +32-2-728-2278  
**Mail:** Honeywell PACE TAC  
Avenue du Bourget, 1  
B-1140 Brussels, Belgium

### Pacific

**Contact:** Honeywell Global TAC - Pacific  
**Phone:** 1300-300-4822 (toll free within Australia)  
+61-2-9353-7255 (outside Australia)  
**Facsimile:** +61-2-9353-8044  
**Mail:** Honeywell Global TAC - Pacific  
5 Thomas Holt Drive  
North Ryde, NSW, 2113, Australia  
**Email** GTAC@honeywell.com

## **India**

**Contact:** Honeywell Global TAC - India  
**Phone:** +91-20-687-5531  
**Facsimile:** +91-20-687-9404  
**Mail:** TATA Honeywell Ltd.  
55 A8 & 9, Hadapsar Industrial  
Hadapsar, Pune -411 013, India  
**Email** Global-TAC-India@honeywell.com

## **Korea**

**Contact:** Honeywell Global TAC - Korea  
**Phone:** +82-2-799-6317  
+82-11-743-6016  
**Facsimile:** +82-2-792-9015  
**Mail:** Honeywell IAC SBE, CRC  
17F, Kikje Center B/D,  
191, Hangangro-2Ga  
Yongsan-gu, Seoul, 140-702, Korea  
**Email** Global-TAC-Korea@honeywell.com

## **People's Republic of China**

**Contact:** Honeywell Global TAC - China  
**Phone:** +86-10-8458-3280 ext. 361  
**Mail:** Honeywell Tianjin Limited  
17 B/F Eagle Plaza  
26 Xiaoyhun Road  
Chaoyang District  
Beijing 100016, People's Republic of China  
**Email** Global-TAC-China@honeywell.com

## **Singapore**

**Contact:** Honeywell Global TAC - South East Asia  
**Phone:** +65-580-3500  
**Facsimile:** +65-580-3501  
+65-445-3033  
**Mail:** Honeywell Private Limited  
Honeywell Building  
17, Changi Business Park Central 1  
Singapore 486073  
**Email** GTAC-SEA@honeywell.com

## **Taiwan**

**Contact:** Honeywell Global TAC - Taiwan  
**Phone:** +886-7-323-5900  
**Facsimile:** +886-7-323-5895  
+886-7-322-6915  
**Mail:** Honeywell Taiwan Ltd.  
10F-2/366, Po Ai First Rd.  
Kaohsiung, Taiwan, ROC  
**Email** Global-TAC-Taiwan@honeywell.com

## **Japan**

**Contact:** Honeywell Global TAC - Japan  
**Phone:** +81-3-5440-1303  
**Facsimile:** +81-3-5440-1430  
**Mail:** Honeywell K.K.  
1-14-6 Shibaura Minato-Ku  
Tokyo 105-0023  
Japan  
**Email** Global-TAC-JapanJA25@honeywell.com

## **Elsewhere**

Call your nearest Honeywell office.

## **World Wide Web**

Honeywell Solution Support Online:  
<http://www.ssol.acs.honeywell.com>

## Training classes

Honeywell holds technical training classes on Safety Manager. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see <http://www.automationcollege.com>.

## Related Documentation

The following guides are available for Safety Manager.

The guide in front of you is *Safety Manual*.

Guide	Description
The <i>Overview Guide</i>	This guide describes the general knowledge required, the basic functions of, and the tasks related to Safety Manager.
The <i>Safety Manual</i>	This guide describes the specifications, design guidelines, and safety aspects related to Safety Manager.
The <i>Planning and Design Guide</i>	This guide describes the tasks related to planning and designing a Safety Manager project.
The <i>Installation and Upgrade Guide</i>	This guide describes the tasks related to installing, replacing and upgrading hardware and software as part of a Safety Manager project.
The <i>Troubleshooting and Maintenance Guide</i>	This guide describes the tasks related to troubleshooting and maintaining Safety Manager.
The <i>System Administration Guide</i>	This guide describes the task related to administrating the computer systems used in a Safety Manager project.
The <i>Hardware Reference</i>	This guide specifies the hardware components that build a Safety Manager project.
The <i>Software Reference</i>	This guide specifies the software functions that build a Safety Manager project and contains guidelines on how to operate them.
The <i>On-line Modification Guide</i>	This guide describes the theory, steps and tasks related to upgrading Safety Builder and embedded software and modifying an application online in a redundant Safety Manager.

## Task-oriented guides

A task-oriented guide provides both procedural and basic knowledge. A task can inform the reader on *how to* perform the task in terms of steps to follow.

Additionally a task can describe *what* important considerations to make or what options to choose from when performing a task.

A task-oriented guide lists the required skills and knowledge that people must master to qualify for the described tasks.

It is common for task oriented guides to refer to reference guides for details.

## Reference guides

A reference guide provides detailed information or solutions regarding its scope. A reference guide is a Safety Manager related guide and provides background information to support tasks as described in task-oriented guides.

A reference guide does not describe tasks in terms of *how to* perform the task in terms of steps to follow.

## Available electronic format

All guides are accessible via the Safety Manager Knowledge Builder; an Internet Explorer based viewer with extensive search and indexing options.

The Knowledge Builder contains guides stored as:

- web pages
- Adobe PDF guides

The information stored on the Safety Manager Knowledge Builder CD-ROM can be installed as stand-alone or merged with other Knowledge Builder booksets on a server.

## Conventions

### Symbols

The following symbols are used in Safety Manager documentation:



#### Attention





This symbol is used for information that emphasizes or supplements important points of the main text.



#### Tip

This symbol is used for useful, but not essential, suggestions.

---

	<p><b>Note</b></p> <p>This symbol is used to emphasize or supplement important points of the main text</p>
	<p><b>Caution</b></p> <p>This symbol warns of potential damage, such as corruption of the database.</p>
	<p><b>Warning</b></p> <p>This symbol warns of potentially hazardous situation, which, if not avoided, could result in serious injury or death.</p>
	<p><b>ESD</b></p> <p>This symbol warns for danger of an electro-static discharge to which equipment may be sensitive</p>

### Fonts

The following fonts are used in Safety Manager documentation:

#### *Emphasis*

- “... inform the reader on *how to* perform the task in terms of...”
- “...see the *Overview Guide*”

#### **Label**

“The **Advanced** tab of the **Properties** window has..”

#### **Steps**

Take the following steps:

1. **Create a plant and set its properties.**
2. ....

#### Value

“Low is the fault reaction state for digital inputs and digital outputs.”

#### *Variable*

“The syntax is: **filename** [-s] [-p]“

`http://www.honeywellsms.com`

*Emphasised text* is used to:

- emphasise important words in the text,
- identify document titles.

This font is used to identify labels.

**Labels** are used for Dialog box labels, menu items, names of properties, and so on.

This font is used to identify steps.

**Steps** indicate the course of action that must be adhered to, to achieve a certain goal.

This font is used to indicate a value.

Value is a variable that the reader must resolve by choosing a pre-defined state.

This font is used to identify a variable.

*Variables* are used in syntax and code examples.

This font is used to identify a URL, directing a reader to a website that can be referred to.



# Contents

<b>1 The Safety Manual</b>	<b>1</b>
Content of <i>Safety Manual</i> . . . . .	2
Basic skills and knowledge . . . . .	3
Prerequisite skills. . . . .	3
Training . . . . .	3
Safety standards for Process & Equipment Under Control (PUC, EUC) . . . . .	4
Safety Integrity Level (SIL) . . . . .	4
Equipment Under Control (EUC) . . . . .	4
Process Under Control (PUC) . . . . .	5
Application design conform IEC 61131-3. . . . .	6
The IEC 61508 and IEC 61511 standards . . . . .	7
<b>2 Introduction</b>	<b>9</b>
System overview . . . . .	10
Certification. . . . .	11
Standards compliance . . . . .	13
EU Standards. . . . .	16
CE marking . . . . .	16
EMC directive (89/336/EEC) . . . . .	17
Low voltage directive (73/23/EEC). . . . .	18
Machine safety directive (89/392/EEC)). . . . .	18
Definitions . . . . .	20
<b>3 Safety Manager architectures</b>	<b>29</b>
Safety Manager basic architectures. . . . .	30
Dual Modular Redundant (DMR) architecture . . . . .	30
Quadruple Modular Redundant (QMR) architecture . . . . .	31
System architectures . . . . .	32
Overall safety life cycle. . . . .	39
<b>4 Design phases for an E/E/PE safety-related system</b>	<b>45</b>
Specifying the safety integrity level of the process. . . . .	46
Specifying the field instrumentation . . . . .	47
Specifying the safety-related system functions. . . . .	49
Approval of the specification . . . . .	51

<b>5</b>	<b>Design and implementation phases of Safety Manager</b>	<b>53</b>
	Safety Manager project configuration . . . . .	54
	Safety Manager configuration parameters . . . . .	57
	Specification of input and output signals . . . . .	59
	Implementation of the application software . . . . .	60
	Application verification. . . . .	61
<b>6</b>	<b>Safety Manager special functions</b>	<b>63</b>
	Forcing of IO signals. . . . .	64
	Communication with third party Control systems . . . . .	67
	On-line modification . . . . .	68
<b>7</b>	<b>Safety Manager fault detection and response</b>	<b>69</b>
	Principle of fault detection and response . . . . .	70
	Definitions. . . . .	70
	Principle of fault detection . . . . .	73
	Principle of fault response. . . . .	74
	Watchdog and redundancy . . . . .	78
	Safety Manager alarm markers, registers and diagnostic inputs. . . . .	80
	System markers and registers . . . . .	80
	Alarm markers. . . . .	81
	Diagnostic inputs. . . . .	83
	SM IO faults . . . . .	85
	Digital input faults. . . . .	86
	Analog input faults . . . . .	87
	Digital output faults. . . . .	87
	Analog output faults . . . . .	89
	IO compare errors and system response . . . . .	90
	Compare error detection and synchronization. . . . .	92
	SM Controller faults . . . . .	95
	QPP faults . . . . .	96
	USI faults. . . . .	98
	BKM faults . . . . .	99
	PSU faults . . . . .	100
	Communication faults . . . . .	100
	Calculation errors . . . . .	102
	Rules of thumb with respect to safety and availability . . . . .	105
	IO settings . . . . .	105
	System settings . . . . .	106
<b>8</b>	<b>Using Safety Manager alarm markers and diagnostic inputs</b>	<b>109</b>
	Shutdown at assertion of Safety Manager alarm markers. . . . .	110
	Unit shutdown . . . . .	111
	Diagnostic status exchange with DCS . . . . .	115

<b>9 Fire and gas application example</b>	<b>117</b>
Introduction . . . . .	118
General system and Fire and Gas alarms . . . . .	119
Input loops . . . . .	122
Loop status . . . . .	123
Output loops . . . . .	125
Monitoring for alarm status . . . . .	133
Monitoring for failure status . . . . .	136
Inhibit function . . . . .	138
<b>10 Special requirements for TUV-approved applications</b>	<b>141</b>
<b>List of abbreviations</b>	<b>147</b>
<b>Safety Manager Glossary</b>	<b>149</b>



# Figures

Figure 1	Example FLD layout	6
Figure 2	CE mark	16
Figure 3	Failure model	21
Figure 4	Programmable electronic system (PES): structure and terminology	24
Figure 5	Functional diagram: DMR architecture	31
Figure 6	Functional diagram: QMR architecture	32
Figure 7	Functional diagram: non-redundant Controller, non-redundant IO	33
Figure 8	Non-redundant Controller, non-redundant IO configuration	33
Figure 9	Functional diagram: redundant Controller, non-redundant IO	34
Figure 10	Redundant Controller, non-redundant IO configuration	34
Figure 11	Functional diagram: redundant Controller, redundant IO	36
Figure 12	Redundant Controller, redundant IO configuration	36
Figure 13	Redundant Controller with redundant and non-redundant IO configuration	37
Figure 14	Functional diagram: redundant Controller with redundant and non-redundant IO	38
Figure 15	Overall safety life cycle	39
Figure 16	E/E/PES safety life cycle (in realization phase)	40
Figure 17	Software safety life cycle (in realization phase)	41
Figure 18	Relationship of overall safety life cycle to E/E/PES and software safety life cycles	41
Figure 19	Example of Functional Logic Diagram (FLD)	50
Figure 20	Example of a Safety Builder configurator screen	54
Figure 21	Safety Builder Point Configurator main screen	55
Figure 22	Example of Functional Logic Diagram (FLD)	56
Figure 23	The forcing sequence	64
Figure 24	Schematic diagram of a SMOD with 4 channels	72
Figure 25	Each watchdog has 2 outputs	79
Figure 26	Input failure alarm marker function	83
Figure 27	Intended square-root function	103
Figure 28	Square-root function with validated input value	103
Figure 29	Square-root function with validity check in function block	104
Figure 30	Properties of an analog output module	105
Figure 31	Point detail	106
Figure 32	Diagram to shut down system in case of output compare error	110
Figure 33	Wiring diagram for unit shutdown	111
Figure 34	Functional logic diagram of unit shutdown	113
Figure 35	Safety Manager system information to DCS	115
Figure 36	FLD2000 system alarms	120

## Figures

Figure 37	FLD2002 general fault alarm . . . . .	120
Figure 38	FLD2004 general fire/gas alarm . . . . .	121
Figure 39	FLD530 smoke detector input loop . . . . .	121
Figure 40	FLD120 gas detector input loop . . . . .	122
Figure 41	FLD230 common low level alarm Area 1 . . . . .	123
Figure 42	FLD232 common F&G detector fault Area 1 . . . . .	124
Figure 43	FLD240 sounders and beacons . . . . .	126
Figure 44	FLD290 deluge valve . . . . .	127
Figure 45	FLD162 status signals deluge valve . . . . .	127
Figure 46	FLD160 status signals fire suppression system. . . . .	128
Figure 47	FLD260 start firewater pump(s) . . . . .	129
Figure 48	FLD262 discrepancy alarm firewater pump . . . . .	129
Figure 49	FLD250 alarm signal to PA/GA . . . . .	130
Figure 50	FLD680 HVAC trip signal . . . . .	131
Figure 51	FLD690 close fire damper signals . . . . .	132
Figure 52	FLD250 grouping of alarm signals . . . . .	134
Figure 53	FLD2004 Fire and Gas alarm lamp and buzzer on mimic panel. . . . .	134
Figure 54	FLD240 audible and visual alarm signals . . . . .	135
Figure 55	FLD232 grouping of detector fault signals . . . . .	136
Figure 56	FLD2002 general fault alarm lamp and buzzer on mimic panel. . . . .	137
Figure 57	FLD101 inhibit M-out-of-N function F&G detector devices . . . . .	138
Figure 58	FLD234 common F&G detector inhibited Area 1 . . . . .	139
Figure 59	FLD236 common F&G outputs inhibited Area 1 . . . . .	139
Figure 60	Power supply . . . . .	145
Figure 61	Multidrop link . . . . .	158

# Tables

Table 1	Safety Manager compliance to standards . . . . .	13
Table 2	Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in low demand mode of operation . . . . .	25
Table 3	Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in high demand or continuous mode of operation . . . . .	25
Table 4	Safety Manager architectures . . . . .	30
Table 5	Overall safety life cycle overview. . . . .	42
Table 6	Example specification of IO signals of Safety Manager. . . . .	48
Table 7	Relation between SIL and AK Levels. . . . .	57
Table 8	Example of safety relation of IO signals with location <i>COM</i> . . . . .	67
Table 9	Fault Reaction settings for hardware IO . . . . .	76
Table 10	Fault Reaction settings for communication IO . . . . .	77
Table 11	Safety Manager system markers . . . . .	80
Table 12	Safety Manager system registers. . . . .	81
Table 13	Safety Manager alarm markers . . . . .	81
Table 14	Safety Manager alarm registers. . . . .	82
Table 15	Diagnostic inputs (channel status). . . . .	83
Table 16	Diagnostic inputs (loop status) . . . . .	84
Table 17	Explanation of a “Controller response to faults” table . . . . .	85
Table 18	Controller response to digital input faults . . . . .	86
Table 19	Controller response to analog input faults. . . . .	87
Table 20	Controller response to digital output fault. . . . .	87
Table 21	Controller response to Analog output faults . . . . .	89
Table 22	Explanation of a “Controller response to compare error” table . . . . .	91
Table 23	Controller response to IO compare faults . . . . .	92
Table 24	Explanation of a “response to Controller faults” table . . . . .	96
Table 25	Controller response to QPP faults . . . . .	97
Table 26	Controller response to USI faults . . . . .	99
Table 27	Controller response to BKM faults . . . . .	99
Table 28	Controller response to PSU faults . . . . .	100
Table 29	Controller response to communication faults . . . . .	100





# The *Safety Manual*

# 1

The *Safety Manual* is intended primarily for the people responsible for and performing tasks related to Safety Manager.

This guide provides directions as how to configure and use Safety Manager the way it is intended. It provides design guidelines, lists the boundaries of Safety Manager, and advises the best hardware for certain functions.

Typical readers are all people involved in planning and design, engineering, troubleshooting and maintenance as well as operating Safety Manager.

It is assumed that the reader masters the required skills and knowledge as described herein.

This section contains the following information about this guide:

Topic	See
Content of Safety Manual	page 2
Basic skills and knowledge	page 3
Safety standards for Process & Equipment Under Control (PUC, EUC)	page 4
Application design conform IEC 61131-3	page 6
The IEC 61508 and IEC 61511 standards	page 7



## Note

This guide does not contain information related to other Honeywell Experion PKS systems and third-party controllers such as Allen-Bradley, Series 9000, TDC 3000, Data Hiway, UDC, and so on.

For information about these systems, see the manufacturers bookset.

## Content of *Safety Manual*

The *Safety Manual* guide is a reference guide providing detailed information regarding how safety aspects are met in Safety Manager. A reference guide is a Safety Manager related guide and does not describe tasks in terms of *how to* perform the task in terms of steps to follow. A reference guide can provide input to support decisions required to achieve a certain objective.

Guide	subjects
<i>Safety Manual</i>	<ul style="list-style-type: none"> <li>• “Introduction” on page 9</li> <li>• “Safety Manager architectures” on page 29</li> <li>• “Design phases for an E/E/PE safety-related system” on page 45</li> <li>• “Design and implementation phases of Safety Manager” on page 53</li> <li>• “Safety Manager special functions” on page 63</li> <li>• “Safety Manager fault detection and response” on page 69</li> <li>• “Using Safety Manager alarm markers and diagnostic inputs” on page 109</li> <li>• “Fire and gas application example” on page 117</li> <li>• “Special requirements for TUV-approved applications” on page 141</li> </ul>

## References

The following guides may be required as reference materials:

Guide	Description
<i>The Overview Guide</i>	This guide describes the general knowledge required, the basic functions of, and the tasks related to Safety Manager.
<i>The Planning and Design Guide</i>	This guide describes the tasks related to planning and designing a Safety Manager project.
<i>The Troubleshooting and Maintenance Guide</i>	This guide describes the tasks related to troubleshooting and maintaining Safety Manager.
<i>The System Administration Guide</i>	This guide describes the task related to administrating the computer systems used in a Safety Manager project.
<i>The Hardware Reference</i>	This guide specifies the hardware components that build a Safety Manager project.
<i>The Software Reference</i>	This guide specifies the software functions that build a Safety Manager project and contains guidelines on how to operate them.

---

## Basic skills and knowledge

Before performing tasks related to Safety Manager you need to:

- Understand basic Safety Manager concepts as explained in the *Overview Guide* and the *Glossary*.
- Have a thorough understanding of the *Safety Manual*.
- Have had appropriate training related to Safety Manager that certifies you for your tasks (see the *Planning and Design Guide*).

## Prerequisite skills

When you perform tasks related to Safety Manager, it is assumed that you have appropriate knowledge of:

- Site procedures
- The hardware and software you are working with. These may i.e be: computers, printers, network components, Controller and Station software.
- Microsoft Windows operating systems.
- Programmable logic controllers (PLCs).
- Applicable safety standards for Process & Equipment Under Control.
- Application design conform IEC 61131-3.
- The IEC 61508 and IEC 61511 standards.

This guide assumes that you have a basic familiarity with the process(es) connected to the equipment under control.

## Training

Most of the skills mentioned above can be achieved by appropriate training. For more information, contact your Honeywell SMS representative or see:

- <http://www.honeywellsms.com> or
- <http://www.automationcollege.com>.

## Safety standards for Process & Equipment Under Control (PUC, EUC)

Safety Manager is a PLC based Safety Instrumented System (SIS) performing specific safety functions to ensure risks are kept at predefined levels.

A SIS measures, independently from the Basic Process Control System, a couple of relevant process signals like temperature, pressure, level in a tank or the flow through a pipe. The values of these signals are compared with the predefined safe values, and if needed, the SIS gives an alarm or takes action. *In such cases the SIS controls the safety of the process and lowers the chance of an unsafe situation.*

The logic in Safety Manager defines the response to process parameters.

In this context the following terms are explained in this section:

- Safety Integrity Level (SIL)
- Equipment Under Control (EUC)
- Process Under Control (PUC)

### Safety Integrity Level (SIL)

The IEC 61508 standard specifies 4 levels of safety performance for safety functions. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity, and safety integrity level 4 (SIL4) the highest level. If the level is below SIL 1, the IEC 61508 and IEC 61511 do not apply.

Safety Manager can be used for processes requiring a SIL1, SIL2 and SIL3.

To achieve the required safety integrity level for the E/E/PE safety-related systems, an overall safety life cycle is adopted as the technical framework (as defined in IEC 61508). For more information see inside the *Safety Manual*.

### Equipment Under Control (EUC)

EUC is the equipment controlled by Safety Manager.

Safety-related systems are designed to prevent the EUC from going into a dangerous state. Safety-related systems can broadly be divided into:

- Emergency shutdown systems.
- Fire and Gas detection and control systems.

Safety-related systems interface with the process through sensors and actuators. The required safety integrity level may be achieved by implementing the safety

functions in the process control system or by using separate and independent systems dedicated to safety.

During the various phases of the safety cycle different knowledge and skills are required with respect to EUC. For more information see inside the *Safety Manual*.

## **Process Under Control (PUC)**

A Process Under Control is Equipment Under Control expanded with additional regulations for the process (i.e. refining).

- Where EUC is concerned, the emphasis is on keeping the equipment safe.
- Where PUC is concerned, the emphasis is on keeping the process safe (broader perspective).

Where PUC is concerned, Safety Manager monitors the process for abnormal situations. Safety Manager is able to initiate safety actions and process alarms. An alarm can be caused by abnormal situations in the:

- Process
- Safety loops
- Safety system itself

# Application design conform IEC 61131-3

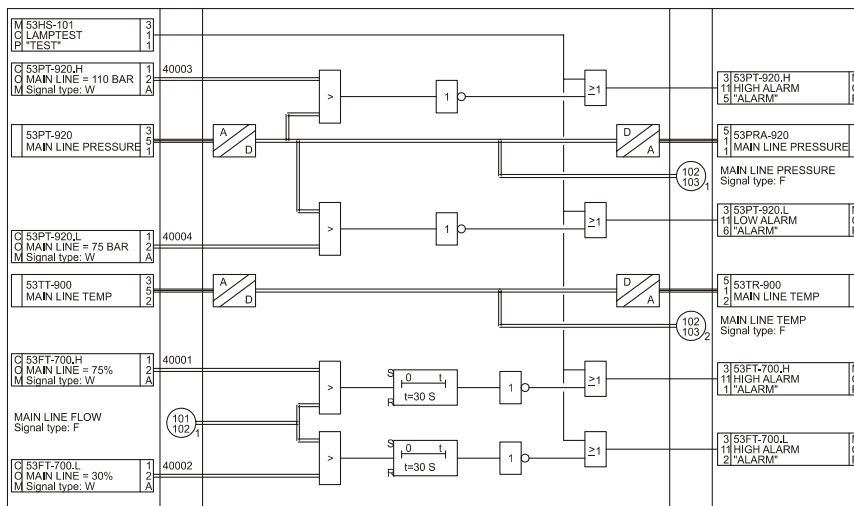
The IEC 61131 standard defines, as a minimum set, the basic programming elements, syntactic and semantic rules for the most commonly used programming languages, including graphical languages of:

- Ladder Diagram,
- Functional Block Diagram and,
- Textual languages of Instruction List and structured Text;

For more information see the IEC web site.

Figure 1 on page 6 shows how Safety Manager uses the graphical programming method, based on Functional Block Diagram as defined by the IEC 61131-3.

**Figure 1** Example FLD layout



---

# The IEC 61508 and IEC 61511 standards

SISs have been used for many years to perform safety functions e.g. in chemical, petro-chemical and gas plants. In order for instrumentation to be effectively used for safety functions, it is essential that the instrumentation meets certain minimum standards and performance levels.

To define the characteristics, main concepts and required performance levels, standards IEC 61508 and IEC 61511 have been developed. The introduction of Safety Integrity level (SIL) is one of the results of these standards.

This brief provides a short explanation of each standard. Detailed information regarding IEC 61508 and 61511 can be found on the IEC web site.



## Tip

For more information regarding, or help on, implementing or determining, the applied safety standards for your plant/process please contact your Honeywell affiliate. Our Safety Consultants can help you to e.g.:

- perform a hazard risk analysis
- determine the SIL requirements
- design the Safety Instrumented System
- validate and verify the design
- train your local safety staff

---

## IEC 61508, the standard for all safety related systems

The IEC 61508 is called “*Functional safety of electrical/electronic/programmable electronic safety-related systems*”

IEC 61508 covers all safety-related systems that are electrotechnical in nature (i.e. electromechanical systems, solid-state electronic systems and computer-based systems).

The standard is generic and can be used directly by industry (as a “standalone” standard) and serves as a basis for the development of sector standards (e.g. for the machinery sector, the process sector the nuclear sector, etc.).

## SIL

IEC 61508 details the design requirements for achieving the required Safety Integrity Level (SIL).

The safety integrity requirements for each individual safety function may differ. The safety function and SIL requirements are derived from the hazard analysis and the risk assessment.

The higher the level of adapted safety integrity, the lower the likelihood of dangerous failure of the SIS.

This standard also addresses the safety-related sensors and final elements regardless of the technology used.

### **IEC 61511, the standard for the process industry**

The IEC 61511 is called “*Functional safety - Safety instrumented systems for the process industry sector*”.

This standard addresses the application of SISs for the process industries. It requires a process hazard and risk assessment to be carried out, to enable the specification for SISs to be derived. In this standard a SIS includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

The standard is intended to lead to a high level of consistency in underlying principles, terminology and information within the process industries. This should have both safety and economic benefits.

It is strongly recommended that attention is paid to the IEC 61508 as the IEC 61511 sits within the framework of IEC 61508.



# Introduction

# 2

The *Safety Manual* describes the specifications, design guidelines, and safety aspects related to Safety Manager.

It is created to ensure that the required safety knowledge for designing, engineering and constructing Safety Manager is transferred to the user.

This section describes the following topics:

Topic	See
System overview	page 10
Certification	page 11
Standards compliance	page 13
Definitions	page 20

---

## System overview

Safety Manager is a Safety Instrumented System (SIS). The SIS can be used in a number of different basic architectures (DMR, QMR) depending on the required availability level.

The safety of Safety Manager is obtained through its specific design for these applications. This design includes facilities for self-testing of all Safety Manager modules through software and specialized hardware based on a failure mode effect analysis (FMEA) for each module. Additional software diagnostic routines are included to guarantee proper execution of the hardware. This approach can be classified as software diversity. These features maintain the highest level of safety operation of Safety Manager even in the single-channel configurations. By placing these single-channel versions in parallel, one not only gets safety but also availability: *proven availability*.

Safety Manager and Safety Station from Honeywell SMS provide the means to guarantee optimal safety and availability. To achieve these goals, it is essential that the system is operated and maintained by authorized and qualified staff. If it is operated by unauthorized or unqualified persons, severe injuries or loss of production could be the result. This *Safety Manual* covers the applications of Safety Manager for Safety Integrity Levels (SIL) 1 to 3 in compliance with the international standard IEC 61508.



### Tip

More overview information regarding Safety Manager can be found in the *Overview Guide*.

---

# Certification

The advantage of applying and complying to standards is obvious:

- International standards force companies to evaluate and develop their products and processes according a consistent and uniform way.
- Products certified conform these international standards guarantee a certain degree of quality and product reliability that other products lack.

Since functional safety is the core of the Safety Manager design, the system has been certified for use in safety applications all around the world. Safety Manager has been developed specifically to comply with the IEC61508 functional safety standards, and has been certified by TUV for use in SIL1 to SIL3 applications.

Safety Manager has also obtained certification in the United States for the UL 1998 and ANSI/ISA S84.01 standards.

For a full list of all these and other certifications see “Certification” on page 11.

## Certification

Safety Manager has been certified to comply with the following standards:



**International Electrotechnical Commission (IEC)** — The design and development of Safety Manager are compliant with IEC 61508 (as certified by TUV).



**Instrument Society of America (ISA)** — Certified to fulfill the requirements laid down in ANSI/ISA S84.01.



**CE compliance** — Complies with CE directives 89/336/EEC (EMC) and 73/23/EEC (Low Voltage), 89/392/EEC (Machine Safety)



**European Committee for Standardization** — CEN, CENELEC



**Lloyds Register of Shipping** — Test specification nr 1 (LRS), 96/98/EEC (EEC Marine directive)



**TUV (Germany)** — Certified to fulfill the requirements of SIL3 safety equipment as defined in the following documents: IEC61508, IEC60664-3, EN50156, EN 54-2, EN50178, IEC 60068, IEC 61131-2, IEC 61131-3, IEC60204.



**Canadian Standards Association (CSA)** — Complies with the requirements of the following standards:

- CSA Standard C22.2 No. 0-M982 General Requirements – Canadian Electrical Code, Part II;
- CSA Standard C22.2 No. 142-M1987 for Process Control Equipment.



**Underwriters Laboratories (UL)** — Certified to fulfill the requirements of UL 508, UL 991, UL 1998, and ANSI/ISA S84.01.



**Factory Mutual (FM)** — Certified to fulfill the requirements of FM 3611 and FM3600 (non-incentive field wiring circuits for selected modules and installation in Class 1 Div 2 environments).

## Standards compliance

This subsection lists the standards Safety Manager complies with, and gives some background information on the relevant CE marking (EMC directive and Low Voltage directive).

**Table 1** Safety Manager compliance to standards

Standard	Title	Remarks
IEC61508 (S84.01)	Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety-related systems.	
DIN V 0801 (1/90) and Amendment A (10/94)	Principles for computers in safety-related systems. <i>(German title: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben)</i>	Microprocessor-based safety systems.
VDE 0116 (10/89)	Electrical equipment of furnaces. <i>(German title: Elektrische Ausrüstung von Feuerungsanlagen)</i>	
EN 54 part 2 (01/90)	Components of automatic fire detection systems, Introduction. <i>(German title: Bestandteile automatischer Brandmeldeanlagen)</i>	
EN 50081-2-1994	Electromagnetic compatibility – Generic emission standard, Part 2: Industrial environment.	
EN 50082-2-1995	Electromagnetic compatibility – Generic immunity standard, Part 2: Industrial environment.	
IEC 61010-1-1993	Safety Requirements for Electrical Equipment for Measurement, Control and Laboratory Use, Part 1: General Requirements.	
IEC 61131-2-1994	Programmable controllers. Part 2: Equipment requirements and tests.	
UL 1998	Safety-related software, first edition.	Underwriters Laboratories.
UL 508	Industrial control equipment, sixteenth edition.	Underwriters Laboratories.

**Table 1** Safety Manager compliance to standards

Standard	Title	Remarks
UL 991	Test for safety-related controls employing solid-state devices, second edition.	Underwriters Laboratories.
FM3600, FM 3611 Class I, Division 2, Groups A, B, C & D  Class II, Division 2, Groups F & G	Electrical equipment for use in <ul style="list-style-type: none"> <li>• Class I, Division 2,</li> <li>• Class II, Division 2, and</li> <li>• Class III, Division 1 and 2, hazardous locations.</li> </ul>	Factory Mutual Research.  Applies to the field wiring circuits of the following modules:  SDI-1624, SAI-0410, SAI-1620m, SDIL-1608 and SAO-0220m, and installation of the Controller in these environments.
CSA C22.2	Process control equipment. Industrial products.	Canadian Standards Association No. 142 (R1993).
IEC 60068-1	Basic environmental testing procedures.	
IEC 60068-2-1	Cold test.	0°C (32°F); 16 hours; system in operation; reduced power supply voltage: (–15%): U=20.4 Vdc or (–10%): U=198 Vac.
IEC 60068-2-1	Cold test.	–10°C (14°F); 16 hours; system in operation.
IEC 60068-2-2	Dry heat test.	up to 65°C (149°F); 16 hours; system in operation; increased power supply voltage: (+15%): U=27.6 Vdc or (+10%): U=242 Vac.
IEC 60068-2-3	Test Ca: damp heat, steady state.	21 days at +40°C (104°F), 93% relative humidity; function test after cooling.
IEC 60068-2-3	Test Ca: damp heat, steady state.	96 hours at +40°C (104°F), 93% relative humidity; system in operation.
IEC 60068-2-14	Test Na: change of temperature – withstand test.	–25°C—+55°C (–13°F—+131°F), 12 hours, 95% relative humidity, recovery time: max. 2 hours.

**Table 1** Safety Manager compliance to standards

Standard	Title	Remarks
IEC 60068-2-30	Test Db variant 2: cyclic damp heat test.	+25°C—+55°C (+77°F—+131°F), 48 hours, 80-100% relative humidity, recovery time: 1—2 hours.
IEC 60068-2-6	Environmental testing – Part 2: Tests – Test. Fc: vibration (sinusoidal).	Excitation: sine-shaped with sliding frequency; Frequency range: 10—150 Hz. Loads: <ul style="list-style-type: none"> <li>• 10—57 Hz; 0.075 mm.</li> <li>• 57—150 Hz; 1 G.</li> </ul> Duration: 10 cycles (20 sweeps) per axis. No. of axes: 3 (x, y, z). Traverse rate: 1 oct/min in operation.
IEC 60068-2-27	Environmental testing – Part 2: Tests – Test. Ea: shock.	Half sine shock. 2 shocks per 3 axes (6 in total). Maximum acceleration: 15 G. Shock duration: 11 ms. Safety Manager in operation.

## EU Standards

This section explains the major EU standards that apply to Safety Manager. These standards are:

Topic	See
CE marking	page 16
EMC directive (89/336/EEC)	page 17
Low voltage directive (73/23/EEC)	page 18
Machine safety directive (89/392/EEC)	page 18

### CE marking

The CE mark (see Figure 2 on page 16) is a compliance symbol, which indicates that a product meets the requirements of the EU directives that apply to that product. CE (Conformité Européenne) marking is a legal requirement for selling products in the European Union.

EU directives documentation is issued on the authority of the Council of the European Union. It contains requirements and regulations for certain categories of products or problem areas. The directives apply not only to member countries of the European Union but also to the whole European Economic Area (EEA).

The European directives have the following key objectives:

- Free movement of goods within the EU/EEA geographical regions through harmonization of standards and elimination of trade barriers.
- Safety of persons, their property and of animals.
- Protection of the environment.

Figure 2 CE mark



For control products like Safety Manager, a number of EU directives apply. Safety Manager is compliant with: the Electromagnetic Compatibility (EMC) Directive (89/336/EEC), the Low Voltage Directive (73/23/EEC), Marine Directive (96/98/EEC) and Machine Safety Directive (89/392/EEC). Some are



discussed in more detail below. An item of equipment may only display the CE mark when the equipment satisfies all relevant directives.

## EMC directive (89/336/EEC)

One of the EU directives Safety Manager complies with is the EMC directive, or *Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility* as it is officially called. It “applies to apparatus liable to cause electromagnetic disturbance or the performance of which is liable to be affected by such disturbance” (Article 2).

The EMC directive defines protection requirements and inspection procedures relating to electromagnetic compatibility for a wide range of electric and electronic items.

Within the context of the EMC directive, ‘apparatus’ means all electrical and electronic appliances together with equipment and installations containing electrical and/or electronic components. ‘Electromagnetic disturbance’ means any electromagnetic phenomenon which may degrade the performance of a device, unit of equipment or system. An electromagnetic disturbance may be electromagnetic noise, an unwanted signal or a change in the propagation medium itself.

‘Electromagnetic compatibility’ is the ability of a device, unit of equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.

There are two sides to electromagnetic compatibility: emission and immunity. These two essential requirements are set forth in Article 4, which states that an apparatus must be constructed so that:

1. The generated electromagnetic disturbance does not exceed a level allowing radio and telecommunications equipment and other apparatus to operate as intended.
2. The apparatus has an adequate level of intrinsic immunity of electromagnetic disturbance to enable it to operate as intended.

The EMC directive was originally published in the Official Journal of the European Communities on May 23, 1989. As of January 1, 1996 compliance with the EMC directive is *mandatory* (a legal requirement). All electronic products may now only be marketed in the European Union if they meet the requirements laid down in the EMC directive. This also applies to Safety Manager cabinets.

## Low voltage directive (73/23/EEC)

Safety Manager also complies with the low voltage directive, or *Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of the Member States relating to electrical equipment designed for use within certain voltage limits* as it is officially called. It states that “electrical equipment may be placed on the market only if, having been constructed in accordance with good engineering practice in safety matters in force in the Community, it does not endanger the safety of persons, domestic animals or property when properly installed and maintained and used in applications for which it was made” (Article 2).

The low voltage directive defines a number of principal safety objectives that electrical equipment must meet in order to be considered “safe”.

Within the context of the low voltage directive, ‘electrical equipment’ means any equipment designed for use with a voltage rating of between 50 and 1,000 V for alternating current (AC) and between 75 and 1,500 V for direct current (DC).

The low voltage directive was originally published in the Official Journal of the European Communities on March 26, 1973. It was amended by Council Directive 93/68/EEC. As of January 1, 1997 compliance with the low voltage directive is *mandatory* (a legal requirement). All electronic products may now only be marketed in the European Union if they meet the requirements laid down in the low voltage directive. This also applies to Safety Manager cabinets.

## Machine safety directive (89/392/EEC)

The directive holds the requirements for machinery safety in every country within the European Economic Area (EEA). The Directive applies to all machinery and to safety components. A machine is defined as “an assembly of linked parts or components, at least one of which moves...”

Machinery meeting the requirements of the Directive is required to have the CE symbol clearly affixed to indicate compliance. An item of equipment may only display the CE mark when the equipment satisfies all relevant directives.

The Directive requires the machines manufacturer to produce a Technical File containing documentary evidence that the machinery complies with the directive. The Directive also effectively allows a period of grace in which the file can be assembled after it has been requested by the authorities.

The Directive gives a comprehensive list of the potential hazards (annex I) which may arise from the design and operation of machinery, and gives general instructions on what hazards must be avoided. Detailed requirements are laid out in a series of safety standards.

Because so many standards are required to cover the full range of machines within the scope of the Directive, the European standards bodies devised a hierarchy which can be applied in every situation:

- ‘Type A’ are the most basic standards set out the requirements for the safety of machines only in the most general terms: part 2 of EN292 is essentially a reproduction of annex 1 of the Machinery Directive.
- ‘Type B’ standards deal with more specific issues: design of emergency stops (EN418); prevention of unexpected start-up (EN1037); pneumatic systems (EN983); temperature of touchable surfaces (EN563) and many others.
- ‘Type C’ standards deal with specific classes of machinery: for example, EN1012 deals with safety of compressors and vacuum pumps; EN 792 deals with pneumatic hand tools.

---

## Definitions

This section provides a list of essential safety terms that apply to Safety Manager. All definitions have been taken from IEC 61508-4, published in 2000.

### Dangerous failure

Failure which has the potential to put the safety-related system in a hazardous or fail-to-function state.



#### Note

Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to-function state.

---

### Error

Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.

### EUC risk

Risk arising from the EUC or its interaction with the EUC control system.

### Failure

The termination of the ability of a functional unit to perform a required function.



#### Note

- The definition in IEC 61508-4 is the same, with additional notes.
  - See Figure 3 on page 21 for the relationship between faults and failures, both in IEC 61508 and IEC 61509.
  - Performance of required functions necessarily excludes certain behavior, and some functions may be specified in terms of behavior to be avoided. The occurrence of such behavior is a failure.
  - Failures are either random (in hardware) or systematic (in hardware or software).
-

## Fault

Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.



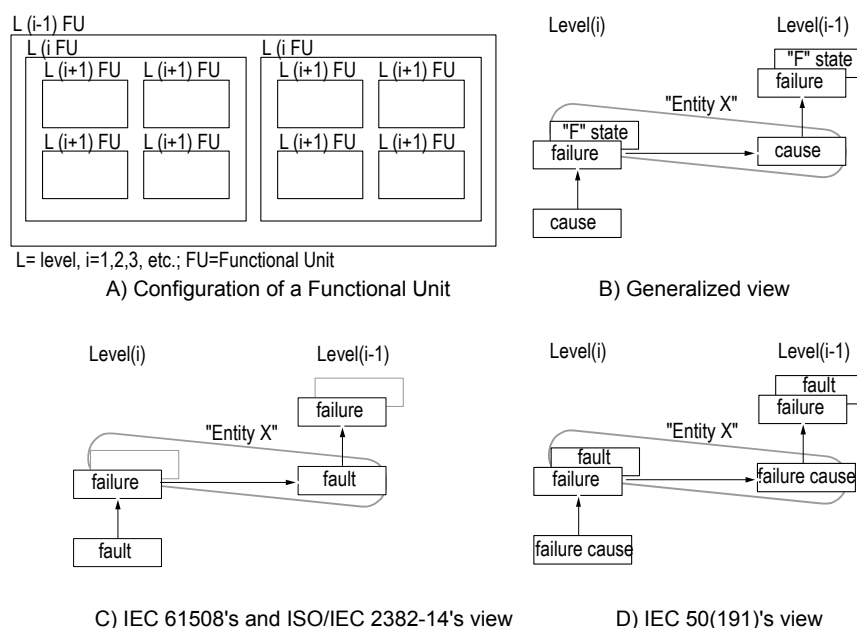
### Note

IEV 191-05-01 defines “fault” as a state characterized by the inability to perform a required function, excluding the inability during preventative maintenance or other planned actions, or due to lack of external resources.

## Functional safety

Part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.

**Figure 3** Failure model





#### Notes for Figure 3 on page 21

- As shown in A), a functional unit can be viewed as a hierarchical composition of multiple levels, each of which can in turn be called a functional unit. In level (i), a “cause” may manifest itself as an error (a deviation from the correct value or state) within this level (i) functional unit, and, if not corrected or circumvented, may cause a failure of this functional unit, as a result of which it falls into an “F” state where it is no longer able to perform a required function (see B)). This “F” state of the level (i) functional unit may in turn manifest itself as an error in the level (i-1) functional unit and, if not corrected or circumvented, may cause a failure of this level (i-1) functional unit.
- In this cause and effect chain the same thing (“Entity X”) can be viewed as a state (“F” state) of the level (i) functional unit into which it has fallen as a result of its failure, and also as the cause of the level (i-1) functional unit. This “Entity X” combines the concept of “fault” in IEC 61508 and ISO/IEC 2382-14, which emphasizes its cause aspect as illustrated in C), and that of “fault” in IEC 50(191), which emphasizes its state aspect as illustrated in D). The “F” state is called fault in IEC 50(191), whereas it is not defined in IEC 61508 and ISO/IEC 2382-14.
- In some cases, a failure may be caused by an external event such as lightning or electrostatic noise, rather than by an internal fault. Likewise, a fault (in both vocabularies) may exist without a prior failure. An example of such a fault is a design fault.

### Functional safety assessment

Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities.

### Human error

Mistake.

Human action or inaction that produces an unintended result.

### Hardware safety integrity

Part of the safety integrity of the safety related systems relating to random hardware failures in a dangerous mode of failure.



#### Note

The term relates to failures in a dangerous mode. That is, those failures of a safety-related system that would impair its safety integrity. The two parameters that are relevant in this context are the overall dangerous failure rate and the probability of failure to operate on demand. The former reliability parameter is used when it is necessary to maintain continuous control in order to maintain safety, the latter reliability parameter is used in the context of safety-related protection systems.

## Mode of operation

Way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it in relation to the proof check frequency, which may be either:

- **Low demand mode** - where the frequency of demands for operation made on a safety-related system is not significantly greater than the proof check frequency; or
- **High demand or continuous mode** - where the frequency of demands for operation made on a safety-related system is significantly greater than the proof check frequency.



### Note

Typically for low demand mode, the frequency of demands on the safety-related system is the same order of magnitude as the proof test frequency (i.e. months to years where the proof test interval is a year). While typically for high demand or continuous mode, the frequency of demands on the safety-related system is hundreds of times the proof test frequency (i.e. minutes to hours where the proof test interval is a month).

---

## Programmable electronic system (PES)

System for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices (see Figure 4 on page 24).

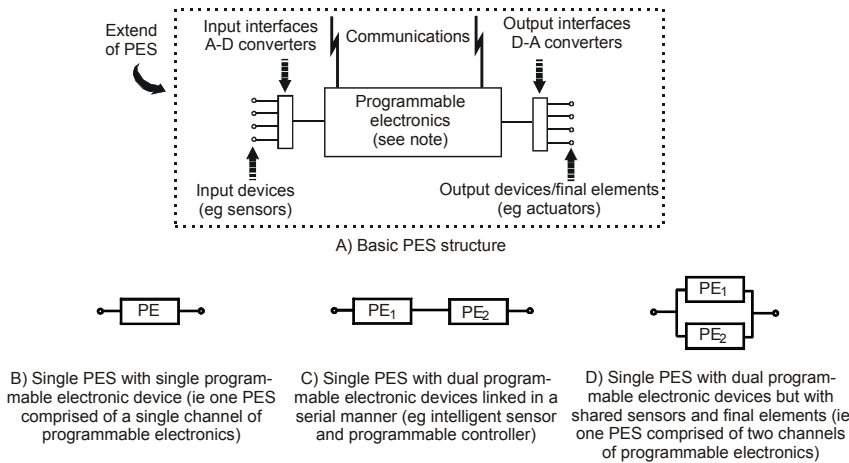


### Note

The structure of a PES is shown in Programmable electronic system (PES): structure and terminology A). Programmable electronic system (PES): structure and terminology B) illustrates the way in which a PES is represented in IEC 61508, with the programmable electronics shown as a unit distinct from sensors and actuators on the EUC and their interfaces, but the programmable electronics could exist at several places in the PES. Programmable electronic system (PES): structure and terminology C) illustrates a PES with two discrete units of programmable electronics. Programmable electronic system (PES): structure and terminology D) illustrates a PES with dual programmable electronics (i.e. two channel), but with a single sensor and a single actuator.

---

**Figure 4** Programmable electronic system (PES): structure and terminology




**Risk**

Combination of the probability of occurrence of harm and the severity of that harm.

**Safe failure**

Failure which does not have the potential to put the safety-related system in a hazardous or fail-to-function state.

	<p><b>Note</b></p> <p>Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a safe hardware failure is less likely to result in an erroneous shutdown.</p>
---	--

**Safety**

Freedom from unacceptable risk.

**Safety integrity level (SIL)**

Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related



systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.



#### Note

- The target failure measures for the safety integrity levels are specified in Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in low demand mode of operation and Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in high demand or continuous mode of operation.

**Table 2** Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in low demand mode of operation

Safety integrity level	Low demand mode of operation (average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE: see notes below for details on interpreting this table.	

**Table 3** Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in high demand or continuous mode of operation

Safety integrity level	High demand or continuous mode of operation (probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE: see notes below for details on interpreting this table.	



#### Note

1. The parameter in Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in high demand or continuous mode of operation, probability of a dangerous failure per hour, is sometimes referred to as the frequency of dangerous failures, or dangerous failure rate, in units of dangerous failures per hour.
2. This document sets a lower limit on the target failure measures, in a dangerous mode of failure, than can be claimed. These are specified as the lower limits for safety integrity level 4 (that is an average probability of failure of  $10^{-5}$  to perform its design function on demand, or a probability of a dangerous failure of  $10^{-9}$  per hour). It may be possible to achieve designs of safety-related systems with lower values for the target failure measures for non-complex systems, but it is considered that the figures in the table represent the limit of what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.
3. The target failure measures that can be claimed when two or more E/E/PE safety-related systems are used may be better than those indicated in Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in low demand mode of operation and Safety integrity levels: target failure measures for a safety function, allocated to the E/E/PE Safety Related System operating in high demand or continuous mode of operation providing that adequate levels of independence are achieved.
4. It is important to note that the failure measures for safety integrity levels 1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to meet the target failure measures with respect to the systematic safety integrity.
5. The safety integrity requirements for each safety function shall be qualified to indicate whether each target safety integrity parameter is either:
  - the average probability of failure to perform its design function on demand (for a low demand mode of operation); or
  - the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

## Safety life cycle

Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.

## Safety-related system

Designated system that both:

- implements the required safety functions necessary to achieve or maintain a safe state for the EUC, and

- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions.



#### Note

1. The term refers to those systems, designated as safety-related systems, that are intended to achieve, together with the external risk reduction facilities, the necessary risk reduction in order to meet the required tolerable risk.
2. The safety-related systems are designed to prevent the EUC from going into a dangerous state by taking appropriate action on receipt of commands. The failure of a safety-related system would be included in the events leading to the identified hazard or hazards. Although there may be other systems having safety functions, it is the safety-related systems that have been designated to achieve, in their own right, the required tolerable risk. Safety-related systems can broadly be divided into safety-related control systems and safety-related protection systems, and have two modes of operation.
3. Safety-related systems may be an integral part of the EUC control system or may interface with the EUC by sensors and/or actuators. That is, the required safety integrity level may be achieved by implementing the safety functions in the EUC control system (and possibly by additional separate and independent systems as well) or the safety functions may be implemented by separate and independent systems dedicated to safety.
4. A safety-related system may:
  - be designed to prevent the hazardous event (that is if the safety-related systems perform their safety functions then no hazard arises). The key factor here is the ensuring that the safety-related systems perform their functions with the degree of certainty required (for example, for the specified functions, that the average probability of failure should not be greater than  $10^{-4}$  to perform its design function on demand).
  - be designed to mitigate the effects of the hazardous event, thereby reducing the risk by reducing the consequences. As for the first item in this list, the probability of failure on demand for the specified functions (or other appropriate statistical measure) should be met.
  - be designed to achieve a combination of both kinds of systems.
5. A person can be part of a safety-related system. For example, a person could receive information from a programmable electronic device and perform a safety task based on this information, or perform a safety task through a programmable electronic device.
6. The term includes all the hardware, software and supporting services (for example power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements (actuators) and other output devices are therefore included in the safety-related system).
7. A safety-related system may be based on a wide range of technologies including electrical, electronic, programmable electronic, hydraulic and pneumatic.

## Systematic safety integrity

Part of the safety integrity of safety-related systems relating to systematic failures in a dangerous mode of failure.



### Note

Systematic safety integrity cannot usually be quantified (as distinct from hardware safety integrity which usually can).

---

## Validation

Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

# Safety Manager architectures

# 3

To optimize Safety Manager for multiple processes (i.e. batch processing and continues processing), the system can be supplied in a number of architectures, each with its own characteristics and typical applications.

This section provides information on the Safety Manager architectures. It covers the following topics:

Topic	See
Safety Manager basic architectures	page 30
Dual Modular Redundant (DMR) architecture	page 30
Quadruple Modular Redundant (QMR) architecture	page 31

To optimize the choice for a certain system architecture, the availability level is stated next to the type of architecture.

Topic	Availability level	See
System architectures:		page 32
• Non-redundant Controller and non-redundant IO	normal	page 32
• Redundant Controller and non-redundant IO	increased	page 33
• Redundant Controller and redundant IO	optimal	page 35
• Redundant Controller with redundant and non-redundant IO	optimal	page 37

## Safety Manager basic architectures

Safety Manager can be configured for a number of architectures, each with its own characteristics and typical applications. Table 4 on page 30 provides an overview of the available architectures.

**Table 4** Safety Manager architectures

Controller configuration	IO configuration	Remarks
Non-redundant (DMR, see page 30)	Non-redundant, see page 32	DMR architecture; Applications up to SIL3
Redundant (QMR, see page 31)	<ul style="list-style-type: none"> <li>Non-redundant, see page 33</li> <li>Redundant, see page 35</li> <li>Redundant and non-redundant, see page 37</li> </ul>	QMR architecture; Applications up to SIL3

DMR = Dual Modular Redundant

QMR = Quadruple Modular Redundant

All Safety Manager architectures can be used for safety applications. The preferred architecture depends on the availability requirements.

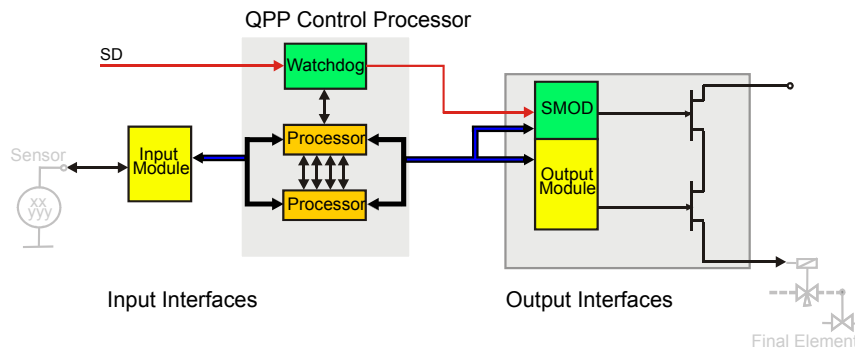
### Dual Modular Redundant (DMR) architecture

Typical applications of a DMR architecture are:

- Burner Management System
- Batch processing
- Machine safety

The Dual Modular Redundant (DMR) architecture provides 1oo2 voting in a non-redundant system. The DMR architecture with 1oo2 voting is based on dual-processor technology, and is characterized by a high level of self tests, diagnostics and fault tolerance.

The DMR architecture is realized with a non-redundant Controller. A non-redundant architecture contains only one QPP (see Figure 5 on page 31), which contains a redundant processor with 1oo2 voting between the processors and memory.

**Figure 5** Functional diagram: DMR architecture

In IO configurations, each path is primarily controlled by the Control Processor and an independent switch (Secondary Means of De-energization, SMOD) which is controlled by an independent watchdog.

## Quadruple Modular Redundant (QMR) architecture

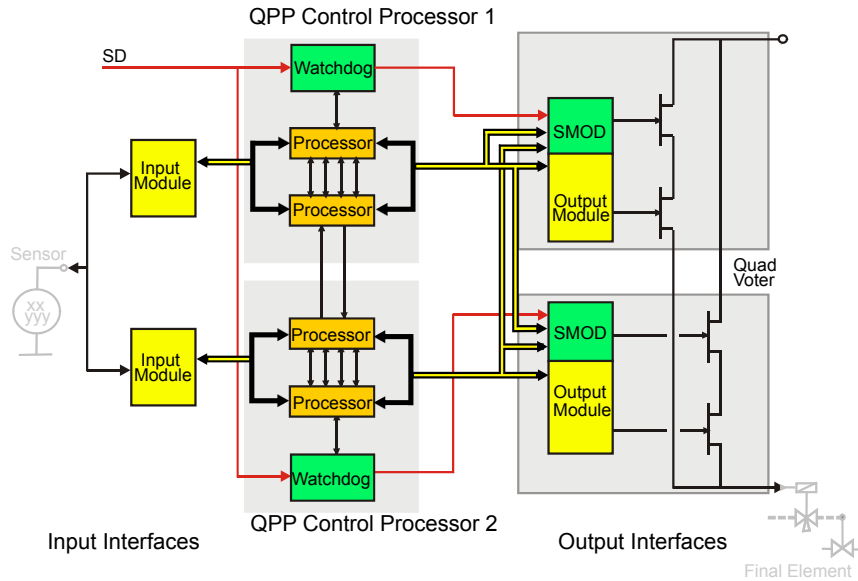
Typical applications of a QMR architecture are:

- process safeguarding applications for which continues operation is essential.

The Quadruple Modular Redundant (QMR) architecture is based on 2oo4D voting, dual-processor technology in each QPP. This means that it is characterized by a ultimate level of self diagnostics and fault tolerance.

The QMR architecture is realized with a redundant Controller. This redundant architecture contains two QPPs (see Figure 6 on page 32), which results in quadruple redundancy making it dual fault tolerant for safety.

The 2oo4D voting is realized by combining 1oo2 voting of both CPUs and memory in each QPP, and 1oo2D voting between the two QPPs. Voting takes place on two levels: on a module level and between the QPPs.

**Figure 6** Functional diagram: QMR architecture

In redundant IO configurations, each path is controlled by one of the Control Processors and an independent switch (Secondary Means of De-energization, SMOD), which is controlled by the diagnostic software and an independent watchdog.

Furthermore, each Control Processor is able to switch off the output channels of the other Control Processor.

## System architectures

### Non-redundant Controller and non-redundant IO

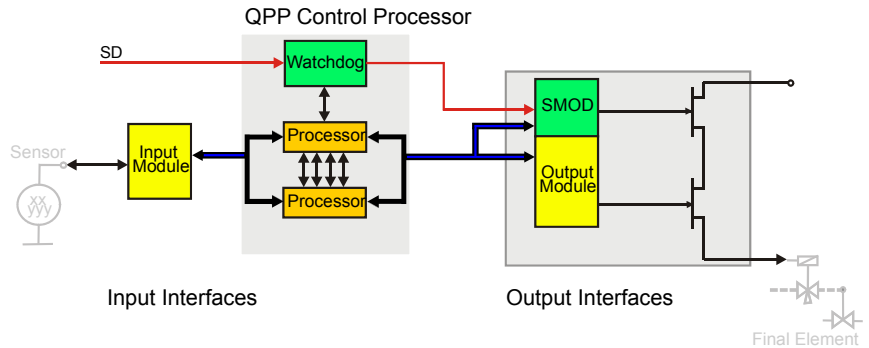
This Safety Manager architecture has a non-redundant Controller and non-redundant input and output (IO) modules (see Figure 8 on page 33 and Figure 7 on page 33).

The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender. There is no redundancy except for those modules with built-in redundancy (QPP, memory and watchdog).

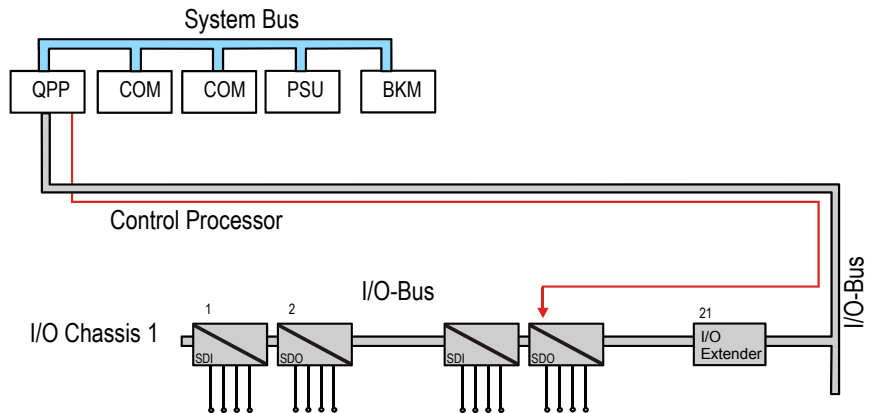
This architecture can be applied up to SIL3.



**Figure 7** Functional diagram: non-redundant Controller, non-redundant IO



**Figure 8** Non-redundant Controller, non-redundant IO configuration



### Redundant Controller and non-redundant IO

This Safety Manager architecture has a redundant Controller and non-redundant input and output (IO) modules (see Figure 10 on page 34 and Figure 9 on page 34).

The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender.

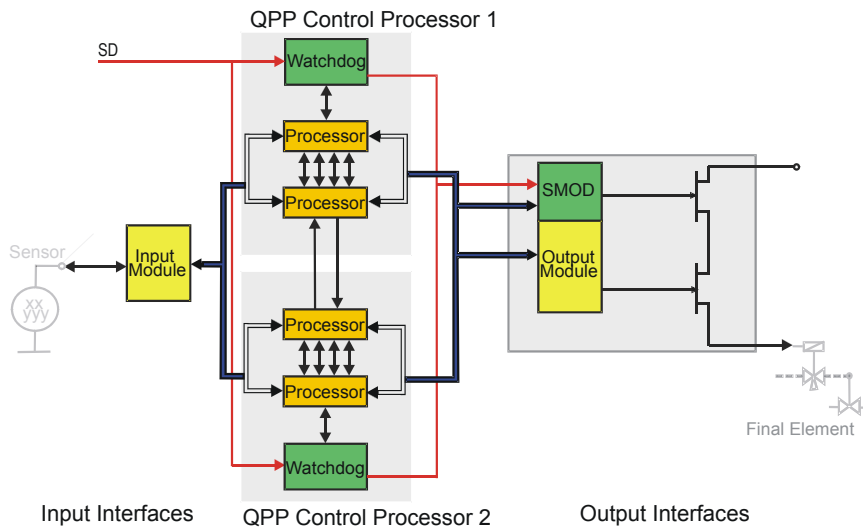
This architecture can be applied up to SIL3.

### Interaction between Control Processors

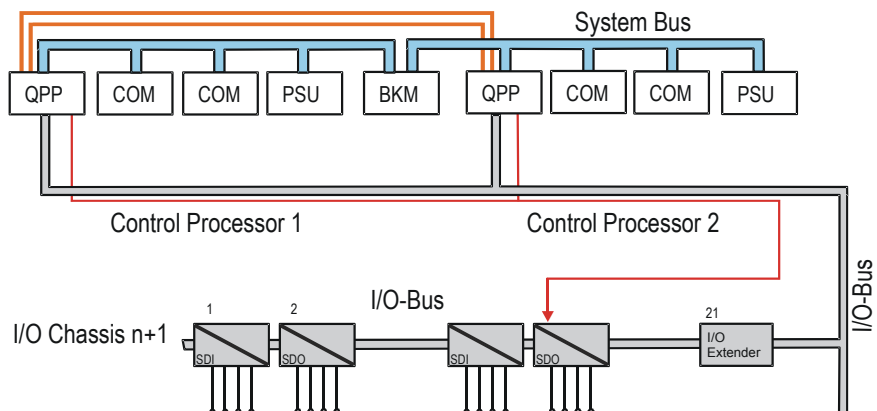
Both Control Processors run in parallel, meaning that they simultaneously read input states and write output states. Via the redundant link both Control Processors continuously inform each other about the achieved IO states, application states. The redundant link is used to synchronize actions and compare results. For more information see “Quadruple Modular Redundant (QMR) architecture” on page 31.

A redundant Controller is single fault tolerant with respect to availability.

**Figure 9** Functional diagram: redundant Controller, non-redundant IO



**Figure 10** Redundant Controller, non-redundant IO configuration



## Redundant Controller and redundant IO

This Safety Manager architecture has a redundant Controller and redundant input and output (IO) modules (OR function outputs) (see Figure 12 on page 36 and Figure 11 on page 36).

The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender. The processor and IO are fully redundant, which allows continuous operation and smooth (zero-delay) transfer of the control in case of a Control Processor or IO failure.

This architecture can be applied up to SIL3.

### Interaction between Control Processors

Both Control Processors run in parallel, meaning that they simultaneously read input states and write output states. Via the redundant link both Control Processors continuously inform each other about the achieved IO states, application states. The redundant link is used to synchronize actions and compare results. For more information see “Quadruple Modular Redundant (QMR) architecture” on page 31.

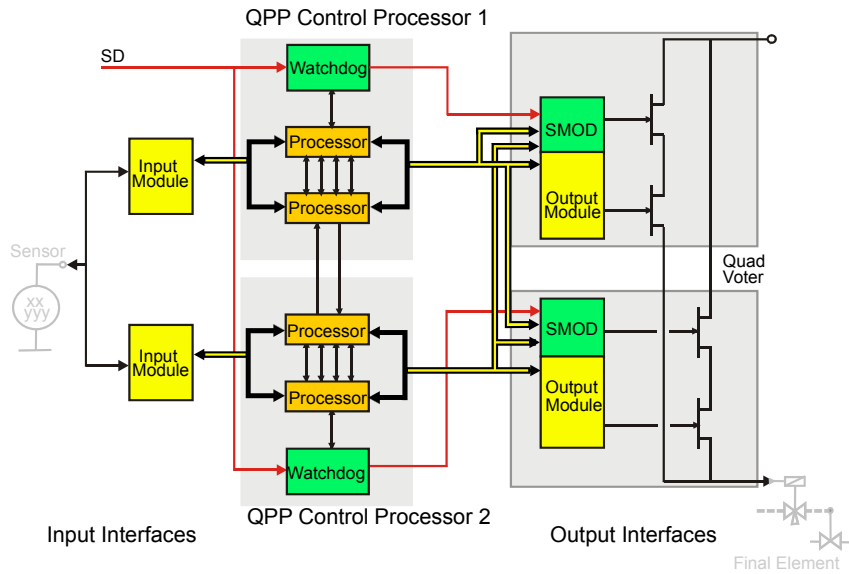
### Interaction between redundant IO

Both IO modules reside next to each other in the same IO chassis. On the backplane they are wired parallel.

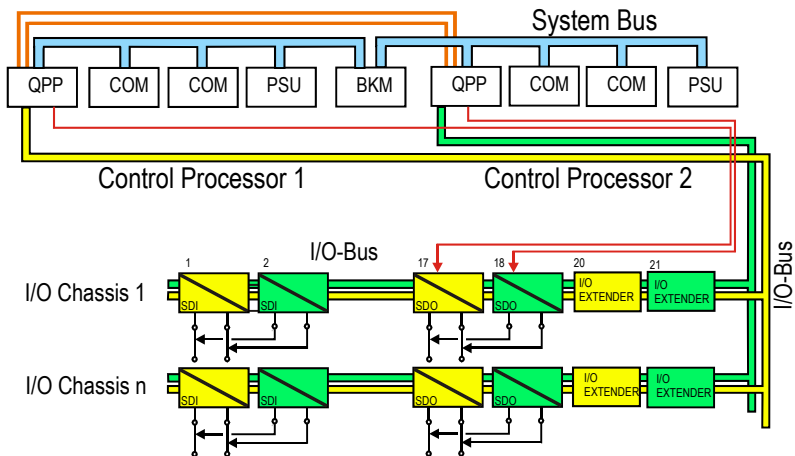
- In principle, when a fault is detected in an input channel, this channel is deactivated by its corresponding Control Processor. The correct value is obtained from the IO module connected to the other Control Processor via the redundant internal link *before* the application cycle is started.
- In principle, when a fault is detected in an output channel, this channel is de-energized by the SMOD (see “Secondary means” on page 25 for details). The correct value is driven into the field by the other Control Processor, but not after both Control Processors have agreed on its value via the redundant internal link.

For more information see “Fault detection and response” on page 23.

**Figure 11** Functional diagram: redundant Controller, redundant IO



**Figure 12** Redundant Controller, redundant IO configuration



## Redundant Controller with redundant and non-redundant IO

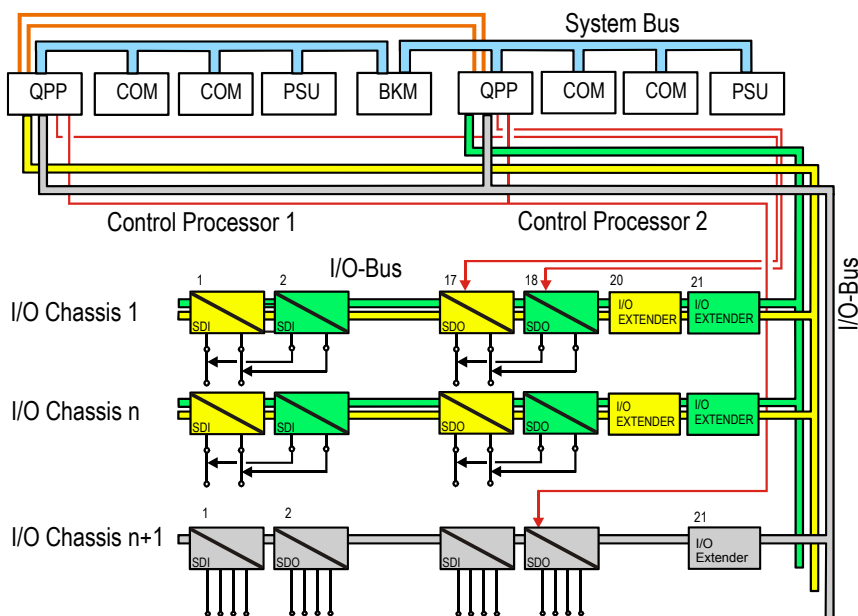
This Safety Manager architecture has a redundant Controller and redundant input and output (IO) modules (OR function outputs) combined with non-redundant input and output modules (see Figure 13 on page 37 and Figure 14 on page 38).

This architecture can be applied up to SIL3.

This architecture is a mix of the described:

- “Redundant Controller and non-redundant IO” on page 33 and
- “Redundant Controller and redundant IO” on page 35.

**Figure 13** Redundant Controller with redundant and non-redundant IO configuration



## Selective watchdog

In a system with combined redundant and non redundant IO 3 watchdog lines are active:

- **WD1**  
This is the Watchdog line dedicated for Control Processor 1.
  - De-energizes upon a safety related fault in Control Processor 1 or an output module of Control Processor 1.
  - When de-energized, Control Processor 1 and the related outputs are halted.

- **WD2**

This is the Watchdog line dedicated for Control Processor 2.

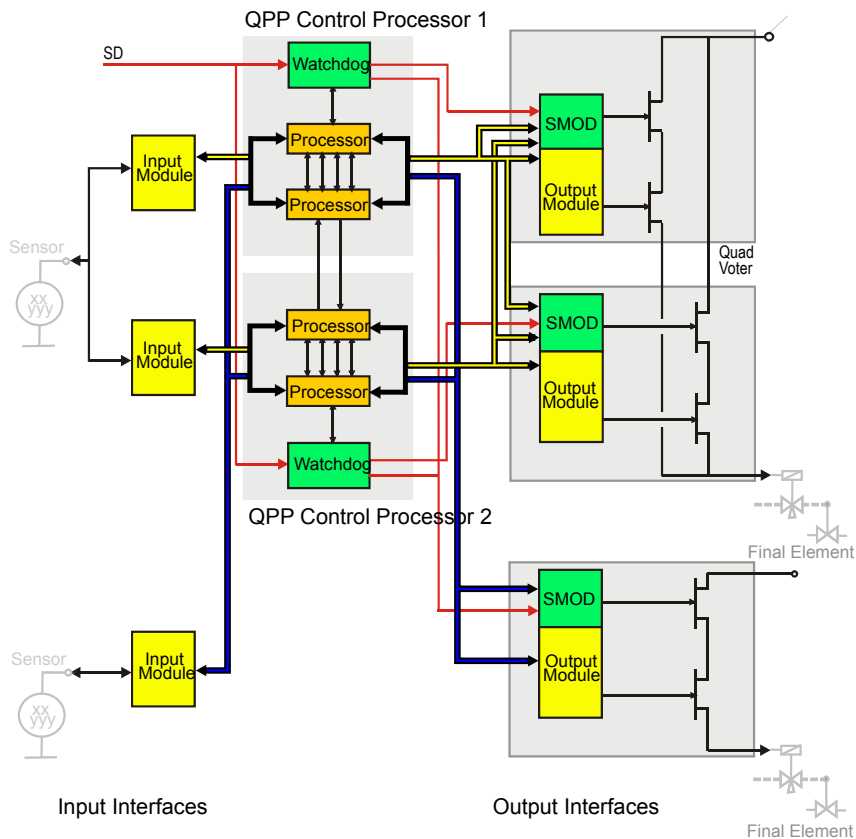
- De-energizes upon a safety related fault in Control Processor 2 or an output module of Control Processor 2.
- When de-energized, Control Processor 2 and the related outputs are halted.

- **WD3**

This is the combined watchdog line, controlled by both Control Processors.

- De-energizes upon a safety related fault in a non redundant output.
- When de-energized, the non-redundant outputs are de-energized, but the redundant outputs and the Control Processors remain operational.

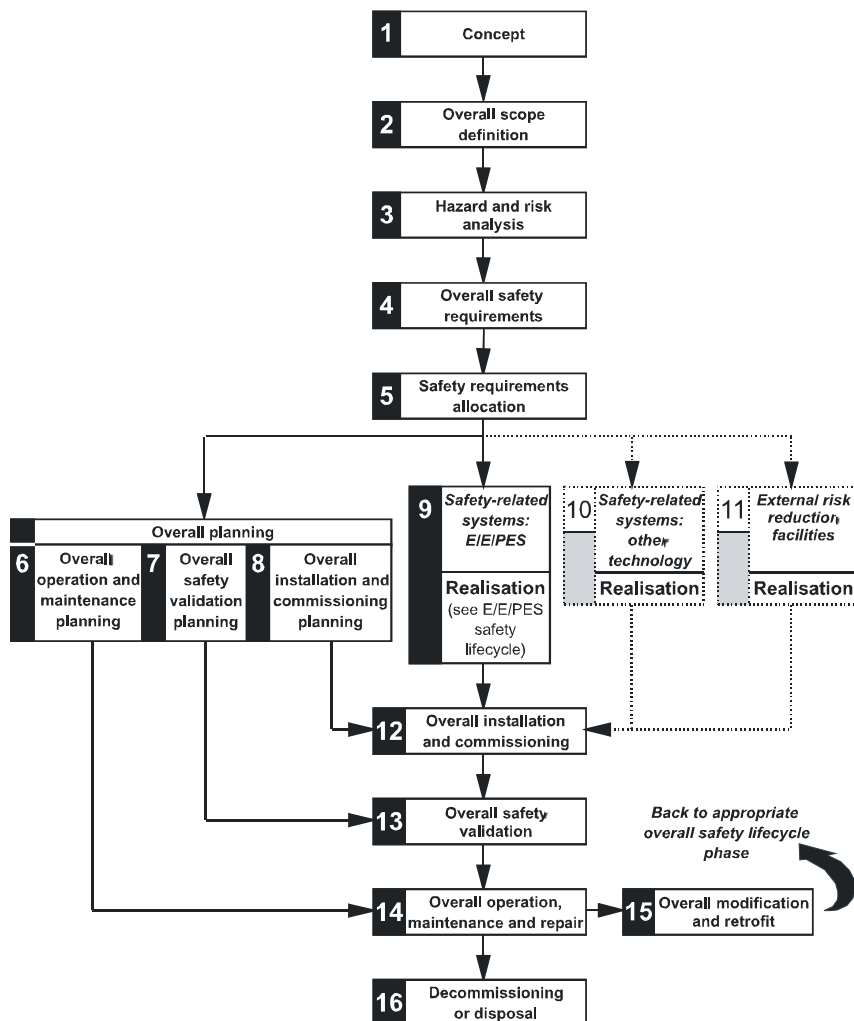
**Figure 14** Functional diagram: redundant Controller with redundant and non-redundant IO



# Overall safety life cycle

To deal in a systematic manner with all the activities necessary to achieve the required safety integrity level for the E/E/PE safety-related systems, an overall safety life cycle is adopted as the technical framework (as defined in IEC 61508) (see Figure 15 on page 39).

**Figure 15** Overall safety life cycle



**Note**

- Activities relating to *verification*, *management of functional safety* and *functional safety assessment* are not shown for reasons of clarity. These activities are relevant to all overall, E/E/PES and software safety life cycle phases.
- The phases represented by boxes 10 and 11 are outside the scope of this standard.
- Parts 2 and 3 deal with box 9 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

The overall safety life cycle encompasses the following risk reduction measures:

- E/E/PE safety-related systems
- Other technology safety-related systems
- External risk reduction facilities

The portion of the overall safety life cycle dealing with E/E/PE safety-related systems is expanded and shown in Figure 16 on page 40. The software safety life cycle is shown in Figure 17 on page 41. The relationship of the overall safety life cycle to the E/E/PES and software safety life cycles for safety-related systems is shown in Figure 18 on page 41.

**Figure 16** E/E/PES safety life cycle (in realization phase)

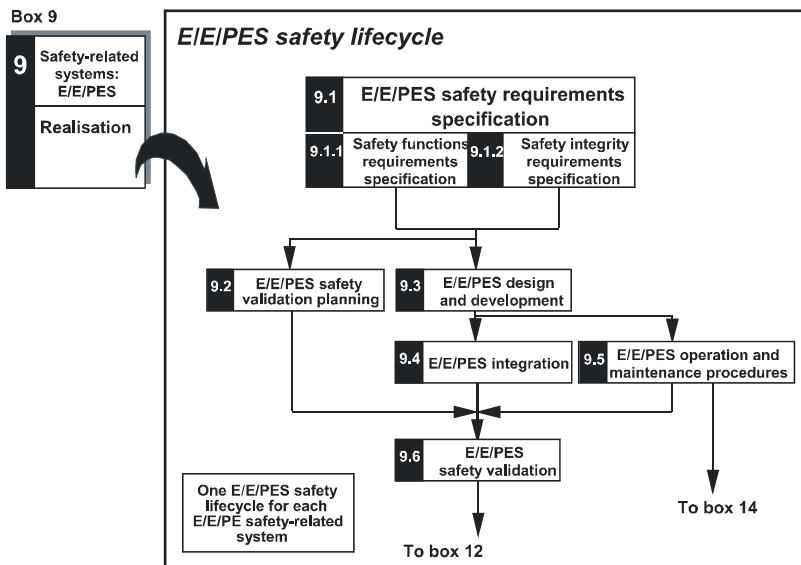




Figure 17 Software safety life cycle (in realization phase)

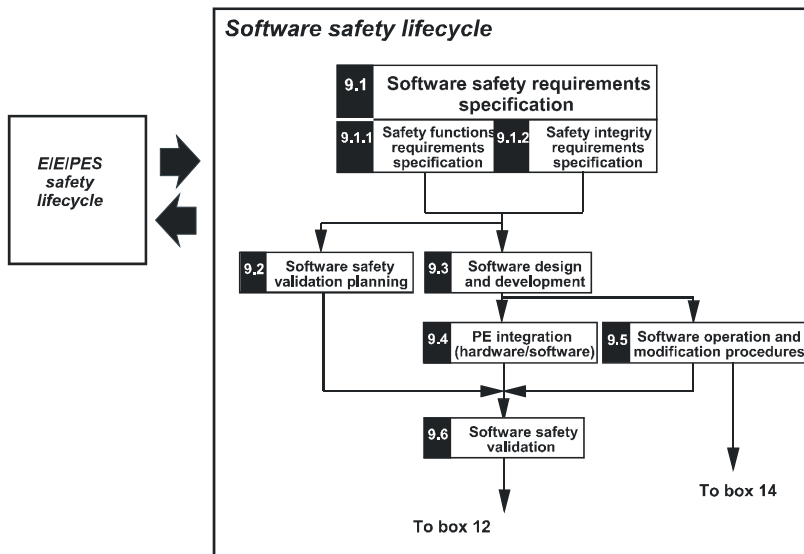
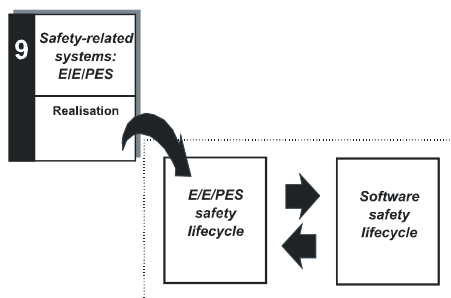


Figure 18 Relationship of overall safety life cycle to E/E/PES and software safety life cycles

Box 9 of overall safety lifecycle



The overall, E/E/PES and software safety life cycle figures (Figure 15 on page 39, Figure 16 on page 40 and Figure 17 on page 41) are simplified views of the reality and as such do not show all the iterations relating to specific phases or between phases. The iterative process, however, is an essential and vital part of development through the overall, E/E/PES and software safety life cycles.

## Objectives

Table 5 on page 42 indicates the objectives to be achieved for all phases of the overall safety life cycle (Figure 16 on page 40).

**Table 5** Overall safety life cycle overview

Phase	Objective	Overall safety life cycle box number
Concept	<ul style="list-style-type: none"> <li>To develop a level of understanding of the EUC and its environment (physical, legislative etc.) sufficient to enable the other safety life cycle activities to be satisfactorily carried out.</li> </ul>	1
Overall scope definition	<ul style="list-style-type: none"> <li>To determine the boundary of the EUC and the EUC control system.</li> <li>To define the scope of the hazard and risk analysis (for example process hazards, environmental hazards, etc.).</li> </ul>	2
Hazard and risk analysis	<ul style="list-style-type: none"> <li>To identify the hazards and hazardous events of the EUC and the EUC control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and misuse.</li> <li>To identify the event sequences leading to the hazardous events identified.</li> <li>To determine the EUC risks associated with the hazardous events identified.</li> </ul>	3
Overall safety requirements	<ul style="list-style-type: none"> <li>To develop the specification for the overall safety requirements to achieve the required functional safety. These specifications contain the safety functions requirements and safety integrity requirements, for the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.</li> </ul>	4
Safety requirements allocation	<ul style="list-style-type: none"> <li>To allocate the safety functions to the designated E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities.</li> <li>To allocate a safety integrity level to each safety function.</li> </ul>	5

**Table 5** Overall safety life cycle overview (*continued*)

Phase	Objective	Overall safety life cycle box number
Overall operation and maintenance planning	<ul style="list-style-type: none"> <li>To develop a plan for operating and maintaining the E/E/PE safety-related systems, to ensure that the required functional safety is maintained during operation and maintenance.</li> </ul>	6
Overall safety validation planning	<ul style="list-style-type: none"> <li>To develop a plan to facilitate the overall safety validation of the E/E/PE safety-related systems.</li> </ul>	7
Overall installation and commissioning planning	<ul style="list-style-type: none"> <li>To develop a plan for the installation of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.</li> <li>To develop a plan for the commissioning of the E/E/PE safety-related systems in a controlled manner, to ensure the required functional safety is achieved.</li> </ul>	8
E/E/PE safety-related systems: realization	<ul style="list-style-type: none"> <li>To create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements.</li> </ul>	9
Other technology safety-related systems: realization	<ul style="list-style-type: none"> <li>To create other technology safety-related systems to meet the safety functions requirements and safety integrity requirements specified for such systems.</li> </ul>	10
External risk reduction facilities: realization	<ul style="list-style-type: none"> <li>To create external risk reduction facilities to meet the safety functions requirements and safety integrity requirements specified for such facilities.</li> </ul>	11
Overall installation and commissioning	<ul style="list-style-type: none"> <li>To install the E/E/PE safety-related systems.</li> <li>To commission the E/E/PE safety-related systems.</li> </ul>	12
Overall safety validation	<ul style="list-style-type: none"> <li>To validate that the E/E/PE safety-related systems meet the specification for the overall safety requirements, taking into account the safety requirements allocation for the E/E/PE safety-related systems.</li> </ul>	13
Overall operation, maintenance and repair	<ul style="list-style-type: none"> <li>To operate, maintain and repair the E/E/PE safety-related systems so that the required functional safety is maintained.</li> </ul>	14
Overall modification and retrofit	<ul style="list-style-type: none"> <li>To ensure that the functional safety of the E/E/PE safety-related systems is appropriate, during and after modification and retrofit activities.</li> </ul>	15

**Table 5** Overall safety life cycle overview (*continued*)

Phase	Objective	Overall safety life cycle box number
Decommissioning or disposal	<ul style="list-style-type: none"> <li>To ensure that the functional safety of the E/E/PE safety-related systems is appropriate in the circumstances during and after the process of decommissioning or disposing of the EUC.</li> </ul>	16

### Sequence of phases

The overall safety life cycle should be used as a basis. The most important item with respect to Safety Manager is the sequence of phases for the works to be done and the decisions to be taken.

The safety-related system connects to the process units, the control system and the operator interface. Consequently, the specification of the safety-related system is made late in the project. However, the first system that is required during start-up and commissioning is the safety system to ensure the safe commissioning of the process unit. The result is always a very tight schedule for the detailed design and production of the safety-related system.

### Self documenting

This requires a flexible safety system that can be easily and quickly engineered and modified without sacrificing or neglecting the safety aspects;  
*self documenting is therefore a prerequisite.*

Safety Manager can be programmed during manufacturing and modified on site through the specification of the safety function (the functional logic diagrams or FLDs). The application program and up-to-date application documentation are generated automatically and almost immediately available.

For details about the design phases with regard to Safety Manager see “Design and implementation phases of Safety Manager” on page 53.

# Design phases for an E/E/PE safety-related system

# 4

This section describes the design phases for an E/E/PE safety-related system. It covers the following topics:

Topic	See
Overall safety life cycle	page 39
Specifying the safety integrity level of the process	page 46
Specifying the field instrumentation	page 47
Specifying the safety-related system functions	page 49
Approval of the specification	page 51

## Specifying the safety integrity level of the process

The overall safety requirements of the safety related system have to be specified according to step 4 of Table 5 on page 42.

Each production process must be classified with regard to safety. Each company shall therefore have competent personnel to conduct SIL classifications. If not available, third party safety consultancy is to be hired.

In Germany for example the government (law) has delegated the approval of both the SIL classification as well as the SIL verification to the TUV.

---

## Specifying the field instrumentation

The field instruments related to the safety-related system consist of valves, limit switches, high-level and low-level pressure switches, temperature switches, flow switches, manual switches, etc. Inputs used for safety applications can be analog or digital. Outputs are mainly digital.

The instrumentation index generally contains:

- Tag number of the instrument
- Description of the process Point
- Make of the instrument
- Supplier
- Setting

### Connections to the safety-related system

The connection to the safety system is specified in the form of a tag number with a description and termination details. The description provides additional information on the tag number and very often includes information on the signal's "health situation" (status).

Following characteristics are to be supported in the IO signal database of a safety system. Table 6 on page 48 shows an extract of the Safety Manager database:

- *Safety Related*  
Indicates whether a signal is to be treated as safety related or not.
- *Force enable*  
Allows forcing of signals (only if certain conditions are met). E.g. for simulation, troubleshooting, maintenance and start-up purposes.
- *Write enable*  
Allows overwriting of communication signals. E.g. to manually change setpoints and flags that are normally controlled by a DCS.

**Table 6** Example specification of IO signals of Safety Manager

Point type	Tag number	Description	Status	Location	Unit	Subunit	Fld number	Safety related	Force Enable	Write Enable
DI	53HS-101	LAMPTTEST	TEST	MCP			102	Yes	Yes	No
DI	53_HS_101	LAMPTTEST	TEST	MCP			104	Yes	Yes	No
DI	91XA-651A	Door switch	Close	AH	5000	91UZ		Yes	No	No
DI	CP_Fault	System marker		SYS			106	Yes	No	No
DI	ExtComFaultCC3	System marker		SYS			106	Yes	No	No
DI	ForceEnable	FORCE-ENABLE	ENABLE	SYS				Yes	No	No
DI	ExtComFaultCC4	System marker		SYS			106	Yes	No	No
DI	Flasher-1Hz	System marker		SYS			107	No	No	No
DI	InputFault	System marker		SYS			122	Yes	No	No
DI	InputForced	System marker		SYS				Yes	No	No
DI	53ES-101	LAMPTTEST		FLD	5000		104	Yes	Yes	No
AI	Sensor-A1	TEMPERATURE		FLD	5000		104	Yes	Yes	No
AO	53PRA-920	MAIN LINE TEMP		FLD	5000		104	No	No	No
DO	53PT-920.H	HIGH ALARM	ALARM	MCP	5000		104	Yes	No	No
BI	53PT-920.H	MAIN LINE= 110BAR		COM	5000		104	No	No	No
BO	Sensor-B3	MAIN LINE TEMP		COM	5000		104	No	No	No

### Determining the signal parameters

The first phase of a safety-related system safety requirements specification is the inventory of the input and output signals, the process interface.

During the specification stage, certain parameters of the IO signal must be determined by the design engineer. For example parameters like the type of signal (digital or analog), safety settings (safety related, force enable etc.), SER enable, scaling, etc.

The setting of the IO parameters determine how Safety Manager treats the inputs and the outputs. This way the design engineer loads the required signal settings, and access restrictions, of each Point in Safety Manager.



---

## **Specifying the safety-related system functions**

The safety functionality of the safety-related system has to be specified according to steps 4 and 5 of Table 5 on page 42:

- Overall safety requirements
- Safety requirements allocation

The basic function of the safety system is to control the outputs (process) according to the predefined logic sequence based on the current state of the process received via the inputs.

The input and output signals of a safety system are a mixture of digital and analog signals. For digital signals, the relation between input and output can be established with various logical functions such as AND, OR and NOT. This is also possible with analog signals when they have been compared with a defined setpoint. To allow certain process conditions to occur or to continue, the safety system requires timing functions (for example delayed on, delayed off, pulse). In Safety Manager, these basic functions have been extended with functionality that allows more complex functions such as counters, calculations, communication, etc.

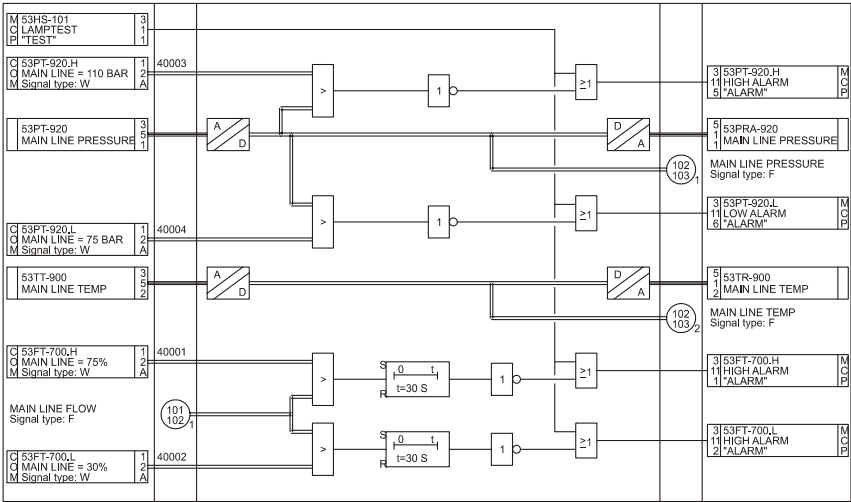
For management purposes a communication link to a supervisory control system may be required. This needs to be specified in this phase of the overall design.

The relations between inputs and outputs have to be chosen so that:

- The process stays in the predefined “operational safe status” during healthy conditions of the input signals.
- The process is directed to a predefined “non-operational safe status” if an unhealthy process or system condition is detected (either automatically or by manual intervention).

The relations between inputs and outputs are determined via functional logic diagrams (FLDs, see Figure 19 on page 50). The functional logic diagrams are created with the Application Editor of the Safety Builder.

Figure 19 Example of Functional Logic Diagram (FLD)



## **Approval of the specification**

The last step is to validate the safety functionality according to steps 4 and 5 of Table 5 on page 42.

This is done by step 7 of Table 5 on page 42:

- Overall safety planning validation

The approved specification is the basis of the design of the safety system. Since the time for the specification preparation is generally too short and since the safety system influences all process units, a large number of revisions (function and termination details) of the specification may be required.

The phases as described in subsections “Specifying the safety integrity level of the process” on page 46 to “Specifying the safety-related system functions” on page 49 are usually performed by the customer or an engineering consultant acting on behalf of the customer. The phases that follow are normally performed by the supplier of the safety system (for example Honeywell SMS for Safety Manager).



# Design and implementation phases of Safety Manager

# 5

This section describes the design and implementation phases when using Safety Manager as a safety-related system.

It briefly describes the Safety Builder options, the toolset available for the engineers to create the application for Safety Manager in a structured way.

The following topics are covered:

Topic	See
Safety Manager project configuration	page 54
Safety Manager configuration parameters	page 57
Specification of input and output signals	page 59
Implementation of the application software	page 60
Application verification	page 61

# Safety Manager project configuration

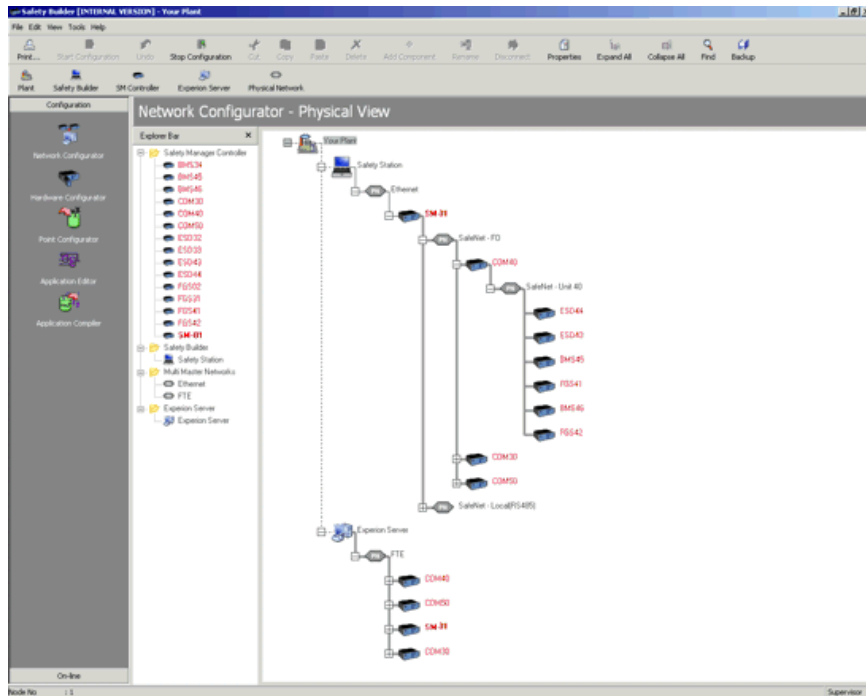
## Safety Builder

To translate the process related safety aspects into a Safety Manager application, the design engineer uses the Safety Builder toolset.

Safety Builder provides a Windows-based user interface to Safety Manager (see Figure 20 on page 54). It is a powerful tool which supports the user in performing a number of design and maintenance tasks. Safety Builder must be used to:

- Configure the network
- Configure Safety Manager
- Design the application program
- Generate application documentation
- Monitor Safety Manager

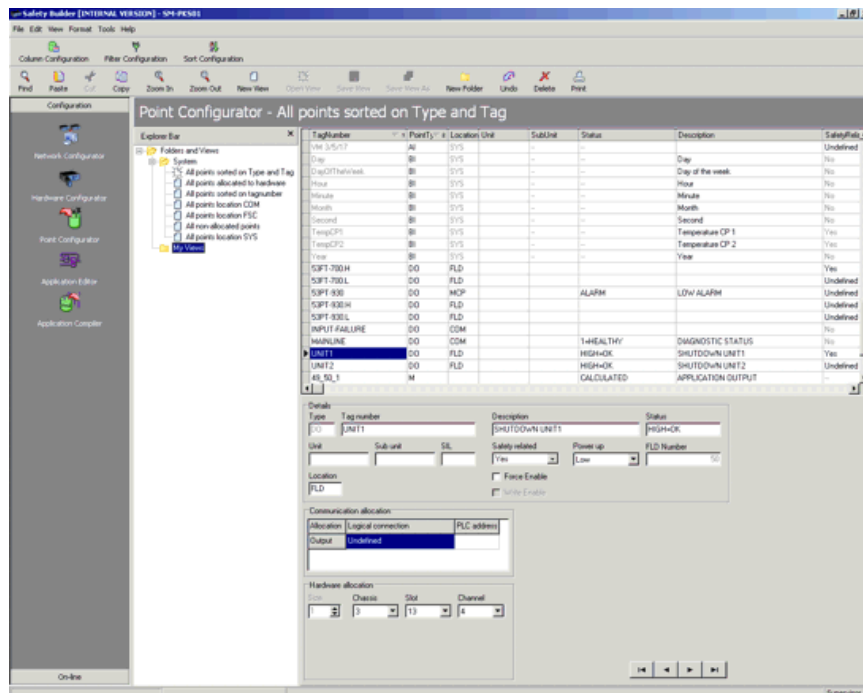
Figure 20 Example of a Safety Builder configurator screen



## Point list

The specification of the IO Points with IO parameters, such as description, hardware configuration, etc. is stored in a Point list as shown in Figure 21 on page 55.

**Figure 21** Safety Builder Point Configurator main screen



The Point list is the basis of the design of the functionality of the safety system by creating functional logic diagrams (FLDs). The use of a Point list containing information on the IO signals has the advantage that basic information only needs to be updated once.

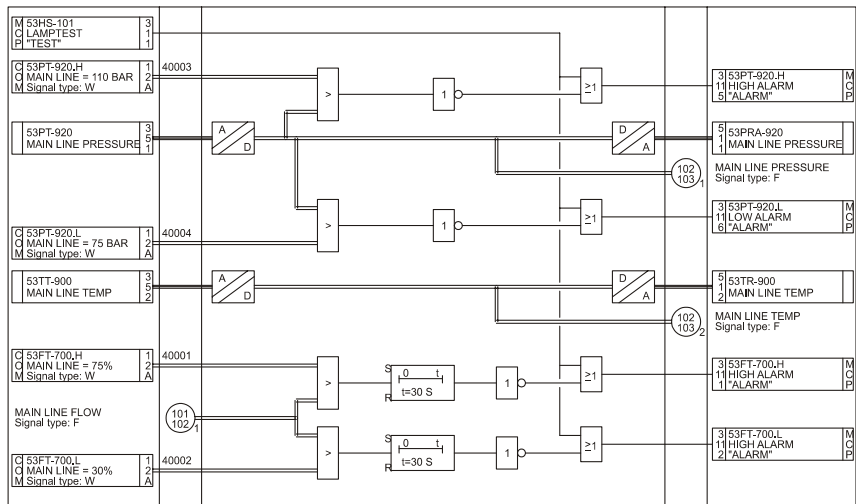
Creating the Point list with aid of the Point Configurator provides:

- A single point of entry for all Point data
- Consistency of throughout the engineering stage
- Automatically updated documentation.

Functional logic diagrams (FLDs)

The functional logic diagrams (FLDs) define the relationship between the inputs and the outputs of a safety system (see Figure 22 on page 56). The information entered in the Point list is added automatically in the functional logic diagrams. The Safety Builder also checks the consistency of the information if the engineer uses Points that have not been allocated to inputs and outputs.

Figure 22 Example of Functional Logic Diagram (FLD)





---

# Safety Manager configuration parameters

## General

The first step in the Safety Manager configuration is to determine the Safety Manager properties.

The most important properties are:

- Safety integrity level
- Safety Manager architecture
- Diagnostic Test Interval
- Interval time between faults

These properties are described in more detail below.

## Safety integrity level

This parameter specifies the level of safety performance of the overall system. Safety Manager supports safety integrity level 1 (SIL1) which is the lowest level of safety integrity through safety integrity level 3 (SIL3) as the highest level. IEC 61508 details the requirements necessary to achieve each safety integrity level. These requirements are more rigorous at higher levels of safety integrity to achieve the required lower likelihood of dangerous failure.

The system safety level can also be expressed in safety requirement classes. DIN V 19250 defines these requirement classes (Anforderungsklassen, or AK). Safety Manager supports AK1 which is the lowest requirement class (low safety level) through AK6 as the highest requirement class (high safety level). Table 7 on page 57 shows the relation between the safety integrity levels and requirement classes.

**Table 7** Relation between SIL and AK Levels

Safety Integrity Level	Safety Requirement Class	Safety Level
SIL1	AK1 - AK3	Low
SIL2	AK4	Medium
SIL3	AK5 and AK6	High

## **Diagnostic Test Interval**

The Diagnostic Test Interval (DTI) is the time a fault may be present in a safety system, without possibly endangering an installation or environment. Therefore it specifies the period in which all self-tests are to be executed within Safety Manager.

## **Maximum repair time**

During normal operation, each Control Processor of Safety Manager performs self-tests and tests the allocated IO modules. If a fault is detected during the tests, the Control Processor reports the failure and takes action to guarantee a safe operational state.

If possible, the fault will be isolated and Control Processor operation continues. If the continuation of the Safe operation cannot be guaranteed, the Control Processor stops. Certain failure types can be isolated, but safe operation can then only be guaranteed as long as no additional faults occur, which, in correlation with the first failure, may lead to unsafe operation. Therefore, when continuing operation, there is a certain risk of such an additional correlating fault occurring. The longer Safety Manager operates, the larger this risk becomes. To keep the risk within acceptable limits, a time interval must be defined: the maximum repair time, which reflects the maximum period of time the Control Processor is allowed to operate after the first failure occurrence. When the maximum repair time expires, the Control Processor shuts down.

The maximum repair time can be defined between 0 and 2047 hours, or can be completely deactivated. In the latter case, organizational measures must be defined to ensure correct action on Safety Manager failure reports.

---

# Specification of input and output signals

## Safety

Safety Builder provides an extensive safety guidance to ensure that correct engineering decisions are taken. Safety Builder assists with allocating IO signals in a safety system. For example, the Point Configurator does not allow multiple allocation or the connection of safety-related signals to modules that do not have self-diagnostic capabilities.

## Input/output signals

The specification of input and output signals is partly done during the specification stage. The data entered in that stage does not contain any information on the physical “chassis/slot/channel” allocation of the IO signal in the safety system.

The Point Configurator of Safety Builder can show Point information of IO signals. To simplify editing and viewing Points, the Point Configurator offers standard and custom views. For detailed information refer to *Software Reference*.

## Physical allocation

The physical allocation of Points in Safety Manager should be chosen based on a number of criteria including:

- Subsystems
- Process units
- Location in the plant
- Type of signal
- Engineering preference

## Implementation of the application software

When the application is built using Safety Builder, the combination of configuration data, Functional Logic Diagrams and Point information can be translated into machine code, which is to be loaded in the SM Controller.

### Translate

Translation of the application into machine code is consists of the following steps:

- 1 The Application Compiler of Safety Builder checks for inconsistencies between:
  - a. System configuration
  - b. IO Point database and
  - c. Functional Logic Diagrams (FLD's)
- 2 Possible errors and warnings are displayed in a log file, which are available and can be printed for future reference.
- 3 If the application proves to be consistent the Application Compiler then generates the machine code and stores it on hard disk.

### Implementation

After the machine code is created, the Controller Management tool is used to load the machine code into the flash memory of the SM Controller (QPP and COM modules). This method does not require any modules to be removed from the chassis.

---

# Application verification

## Introduction

Throughout the application design, several verification steps must be performed to guarantee the actual application software in Safety Manager meets the safety requirements of the process.

## IO signal configuration

The Print option of Safety Builder allows the user to create hard copies of the IO signal configuration as stored in the application database.

The hardcopy must be reviewed to verify that the signal configuration represents the originally defined configuration.

This review may be concentrated on the safety-related configuration aspects, such as the Point qualification, the fault reaction, force enable, hardware allocation and power-on values.

This activity covers the following aspects:

- Data entry by the design engineer.
- System response conform settings in the Hardware Configurator and Point Configurator of Safety Builder.
- Operation of the Safety Station.

Depending on local legislation, the IO signal configuration may need to be approved by an independent certification body, for example TUV.

## Functional logic diagrams (FLDs)

The Print option of Safety Builder also allows the user to create hard copies of the functional logic diagrams as stored in the application database. The hardcopy must be reviewed to verify that the functional logic diagrams represent the intended safeguarding strategy.

This activity covers the following aspects:

- Data entry by the design engineer.
- Operation of the Application Editor of Safety Builder.

Depending on local legislation, the functional logic diagrams may need to be approved by an independent certification body, for example TUV.

## **Application software**

After the application has been successfully translated and the application software has been downloaded to Safety Manager, the correct operation of the application must be verified via a functional test which is carried out during the Factory Acceptance Test (FAT) and/or the start-up and commissioning stages.

The customer then verifies if the original requirements have been correctly implemented in the IO signal configuration, the system configuration and the functional logical diagrams.

## **Functional test**

Functional testing is done via the Application Viewer and a switch box.

Via the switch box, connected to the systems' inputs, the assessor can control the state of each input.

In the Application Viewer the assessor can verify the inputs and application response.

## **Verify load diagnostics**

The Safety Manager File is stored in the SM Controller with the Controller Management function of Safety Builder. After storing, Controller Management reads the diagnostics and checks if the file is correctly stored.

Additionally, an Acceptance Test must be performed. During the Acceptance Test the IO allocation, safety application and communication are tested. This is required to comply with the safety requirements.

# Safety Manager special functions

# 6

This section describes some special functions of Safety Manager. It covers the following topics:

Topic	See
Forcing of IO signals	page 64
Communication with third party Control systems	page 67
On-line modification	page 68

## Forcing of IO signals



### Stop:

Forcing Points can be dangerous if not handled properly! Always communicate your actions when applying or removing forces.

During FAT, on-line testing or calibration of connected devices, it may be required to force an IO Point to a certain fixed state.

For example when testing a defective input sensor forcing allows the sensor to be taken off-line without affecting the continuity of production. While the sensor is being tested, the respective input can be forced to its operational state.

### Enable forcing

The procedure to enable forcing of a Point in Safety Manager is as follows:

- 1 Identify the Points that may require forcing during operation and use the Point Configurator to set the force enable flag of these Points to 'Yes'.
- 2 Translate the application, load it into the system and start the application

### Applying forces

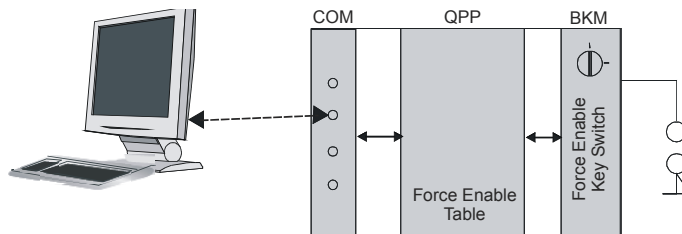


### Warning

Applying forces for a prolonged period of time introduces a potentially dangerous situation as the corresponding process Point could go to the unsafe state while the force is active.

The procedure to apply a force is as follows (see also Figure 23 on page 64):

**Figure 23** The forcing sequence





- 1 Set the *Force Enable* key switch in the “on” position
- 2 Open the Application Viewer with a maintenance engineering user level or above (may be password protected)
- 3 Select the first Point to be forced
- 4 Right click the Point and select a force option from the pop-up menu.

## Setting

IO signals can only be forced using the Application Viewer of Safety Builder. Forcing is only allowed if the correct password has been entered when selecting the force option. The status of the force enable flag is also stored in the application in Safety Manager. This has been done in such a way that a change of the force enable flag after compilation of the application does not allow forcing of the corresponding Point without reloading the application software.

Forces may be set high, low or on a specific value as required. The procedure of how to use forcing is as follows:

- 1 Activate the Force Enable key switch on the BKM after approval by the responsible maintenance manager.
- 2 Use Application Viewer of Safety Builder to select the Point that needs to be forced. (A password may be required.)
- 3 Right click the Point and select the value that the Point should be forced to.
- 4 The force will be applied immediately.



### Notes

- All forces are cleared when the Force Enable key switch is deactivated.
  - All force actions are included in the SER report for review/historical purposes.
- 

## Checks

To make this operation single fault tolerant, both the Safety Builder and the SM Controller carry out checks before a force is executed:

1. Safety Builder checks if the password is activated.
2. Safety Builder checks if the Force Enable key switch is activated.
3. Safety Builder checks if the force enable flag for the Point is set to 'Yes'.
4. SM Controller checks if the Force Enable key switch is activated.
5. SM Controller checks if the force enable flag in the application is set to 'Yes'.

Safety Manager continuously checks the Force Enable key switch and immediately clears all forces when the Force Enable key switch is deactivated.

## Forced Points

If a force command is accepted for an input or output, the ‘*ForceActive*’ system Point becomes active, which can be used as an alarm/indication for operation (see also: “Safety Manager alarm markers, registers and diagnostic inputs” on page 80).

On any subsequent force, the ‘*ForceActive*’ marker pulses for one application cycle. When all forces are cleared, ‘*ForceActive*’ becomes inactive.

## References

Specific TUV requirements with the regard to forcing are described in a document of TUV Bayern Sachsen e.V. and TUV Rheinland: Maintenance override.



### Tip

This document is available on request. Please contact your local Honeywell affiliate or e-mail to [sms-info@honeywell.com](mailto:sms-info@honeywell.com).

---

All Safety Manager architectures meet the requirements specified in this document.

## Clearing forces



### Attention:

To immediately remove *all* forces:

- a. turn the Force Enable key switch or
- b. click the **Remove All Forces** button on the **Application Viewer** tool bar.

### Warning:

This action is irreversible.

---

To remove forces set in Safety Manager, select the forced Point as described in “Setting” on page 65, step 2 onwards.

Instead of selecting a force value, select ‘Clear’. This will clear the force instead of applying a forced value.

# Communication with third party Control systems

## Exchanging process data

Safety Manager can be used to exchange process data with a process control system or PC acting as a man machine interface (e.g. Safety Builder). Such data is represented in functional logic diagrams (FLDs) as Points with location 'COM'.

Points with location 'COM' may only be used for non safety-related functions.

The Point Configurator of Safety Builder sets the safety-relation flag of these signals to 'No' (FALSE) and does not allow this flag to be changed.

The safety-relation flag of the Points can be checked with a list which can be printed with Safety Builder. Table 8 on page 67 shows an example of such an input signal specification.

**Table 8** Example of safety relation of IO signals with location COM

Point type	Tag number	Description	Status	Location	Unit	Subunit	Fld number	Safety related	Force Enable	Write Enable
BI	53PT-920.H	MAIN LINE= 110BAR		COM	5000		104	No	No	No
BO	Sensor-B3	MAIN LINE TEMP		COM	5000		104	No	No	No

## Protocols

For communication with process control systems and computer equipment running visualization programs the Ethernet communication protocols is used.

For details on communication protocols refer to *Planning and Design Guide*.

---

# On-line modification



**Tip:**

Detailed information about On-line modification can be found in *On-line Modification Guide*

---

## Introduction

On-line modification (OLM) is a Safety Manager option which allows you to modify the application software, embedded system software and the Safety Manager hardware configuration of systems with a redundant Controller while the system remains operational.

During the on-line modification, the changes are implemented in the Control Processors one by one. While one Control Processor is being modified, the other Control Processor continues safeguarding the process.

The engineer executing the OLM is guided through the OLM procedure step by step by the Controller Management tool which is integrated in the Safety Builder.

## Compatibility check

During the modification, Safety Manager and the Controller Management tool of the Safety Builder perform a compatibility check of the application-related data, to guarantee a safe changeover from the existing configuration to the new configuration. The system reports the FLD numbers of the changed functional logic diagrams. This allows easy verification of the implemented modifications.

With the Controller Management, changes in the functional logic diagrams (FLDs), the Safety Manager architecture and the system software can be implemented in the system, step by step, without shutting down the system.

For details refer to:

- *Planning and Design Guide*
- *On-line Modification Guide*.

When modifications are implemented in a application, only a functional logic test of the modified functions is required by, for example, TÜV, when the final verification of the implemented changes is obtained via the built-in sheet difference report in Controller Management diagnostics.

# Safety Manager fault detection and response

# 7

A Safety Instrumented System (SIS) is responsible for maintaining the safety of a process or Equipment Under Control (EUC), regardless the state of the system.

Should a fault arise in the SIS, it must deal with this fault in a safe way within the defined Diagnostic Test Interval (DTI).

A Safety Instrumented System operating in Safety Integrity Level 3 (SIL 3) complies if it can detect and safely isolate any single fault within the defined DTI, without affecting the process safety.

This section describes:

- Principles of fault detection and response
- Diagnostic inputs and alarm markers,
- Safety Manager faults,
- Safety Manager response to faults,
- Rules of thumb.

Below table details the topics described in this section:

Topic	See
Principle of fault detection and response	page 70
Safety Manager alarm markers, registers and diagnostic inputs	page 80
SM IO faults	page 85
SM Controller faults	page 95
Calculation errors	page 102
Rules of thumb with respect to safety and availability	page 105

---

## Principle of fault detection and response

The goal of fault detection and response is to detect and isolate any single fault that affects the safety of the process under control, within a time frame that is acceptable for the process.

Below topics describe the principle of fault detection and response.

Topic	See
Definitions	page 70
A Safety Instrumented System (SIS) operating in “high demand mode of operation” must detect and safely isolate any single fault within one PST.	page 73
Watchdog and redundancy	page 78
Watchdog and redundancy	page 78

### Definitions

In order to better understand the concept of fault detection and response a number of related definitions are stated below.

#### Fault reaction

The response to faults in the Controller, application and/or IO.

- The fault reaction towards Controller and/or application faults is fixed.
- The fault reaction towards IO faults can be configured on a module level and should be customized to the application for which Safety Manager is used.

#### Process safety time (PST)

The time a process can be left running uncontrolled without losing the ability to regain control.

#### Diagnostic Test Interval (DTI)

The time period used by Safety Manager to cyclically locate and isolate safety related faults within on-line system components that could otherwise cause a hazardous situation.

With Safety Manager, the default DTI is set at 3 seconds. This setting needs to be verified for each process.

## Repair time

The time allowed to keep a Safety Instrumented System (SIS) running with a fault present that “may affect safety upon accumulation of multiple faults”. Repair time is introduced to extend the SIS up-time for a limited time frame, allowing system repair.

## Repair timer

A configurable count-down timer triggered upon detection of a fault that minimizes the safety availability of the system.

The timer is a configurable count-down timer, which can be deactivated. The default repair window is 200 hours, which is more than sufficient if spare parts are available.

*Each Control Processor has its own repair timer.* Once running, a repair timer shows the remaining time to repair the fault that triggered the repair timer in the Control Processor (200 hours default). If the fault is not repaired within the repair time the Control Processor containing the fault halts.

A repair timer protects the system from certain fault accumulations that may affect the safety of Safety Manager. The timer therefore only starts on detection of faults on output modules and the Force Enable key switch.

## Safe

A design property of an item in which the specified failure mode is predominantly in a safe direction.

## Safety related

A flag to indicate that a signal is used for a safety related function.

## Secondary Means

A means designed to drive towards a safe state in case the primary means is unable or unreliable to do so.

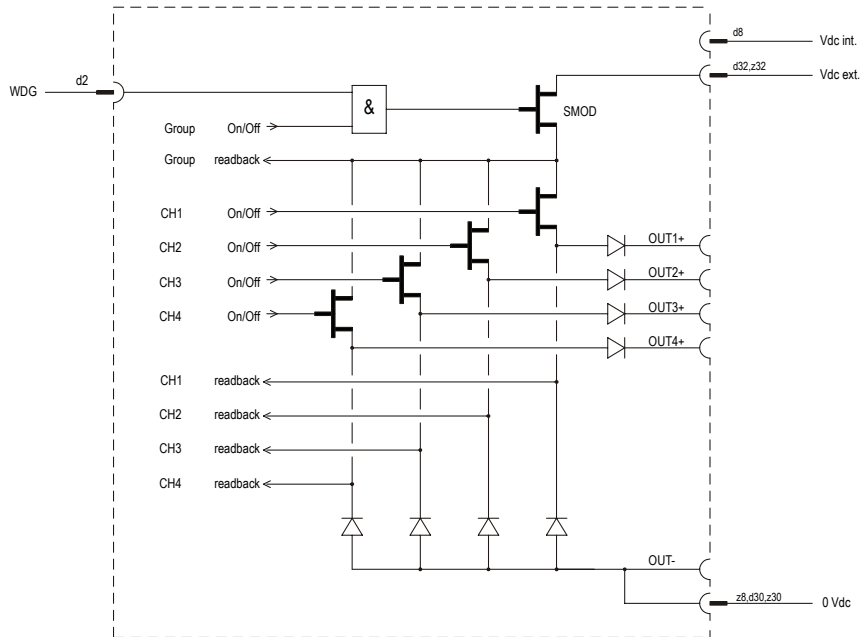
An example of a secondary means is the watchdog: The watchdog is designed to drive the Control Processor and related outputs to a safe state if the Control Processor itself is unable or unreliable to do so.

## Secondary Means Of De-energization (SMOD)

A SMOD is a Secondary Means designed to de-energize the output in case the primary means is unable or unreliable to do so.

Figure 24 on page 72 shows an example of a SMOD protecting 4 output channels.

**Figure 24** Schematic diagram of a SMOD with 4 channels



## Single fault tolerant

Built-in ability of a system to correctly continue its assigned function in the presence of a single fault in the hardware or software.

## Single fault tolerant for safety

Built-in ability of each Safety Manager configuration to continue to maintain safety in the presence of a single fault in the hardware or software.

## Control Processor states

A Control Processor (CP) can have many states. For fault detection and response only the following states are relevant.

- running without detected faults; CP is fully functional and runs the application
- running with detected faults; CP runs the application but lacks certain functions
- halted



The applicable CP state can be read from the User Interface Display located on each Control Processor and from the diagnostic screens available on Experion and Safety Stations.

## IO states

From a SIS point of view, IO can have either the healthy state, the de-energized state or the fault reaction state.

- When healthy, the IO is active and has the application value or a forced value applied.
- When de-energized, the IO is de-activated (as if no power was supplied).
- When the fault reaction state is applied, the IO responds conform a predefined fault condition (fault reaction).

## Process states

A process can have many states. Related to fault detection and response in the safety loop of a process, the following process states are described:

- running without detected faults
- running with detected faults
- halted

## Principle of fault detection

A Safety Instrumented System (SIS) operating in “high demand mode of operation” must detect and safely isolate any single fault within one PST.



### Note

Fault detection and response is aimed at detecting and responding to faults that affect or endanger the *safety* of the system and the process under control.

---

## Fault detection

Fault detection is the first step towards fault response.

Faults in Safety Manager are detected conform the Failure Mode and Effect Analysis (FMEA) model, which provides adequate diagnostics on any detected fault. Test algorithms and / or test circuits are embedded in the safety related software and hardware components, such to allow the detection of these faults.

A running SM Controller continuously performs a series of extensive diagnostic checks on all safety related software and hardware components. This way it will

find faults before they can jeopardize the safety of the process and equipment under control.

### Fault detection cycle

The fault detection and diagnostic checks are executed during a fault detection cycle, which is usually split-up over a number of application cycles.

A fault detection cycle always lasts less than one DTI.

### Fault database

Upon detection, a fault is stored in a fault database, where it is further processed by the Controller.

Upon the severity of the fault, the configuration settings, the redundancy in the Controller and other user settings, the Controller will decide what action is appropriate.

To clear a fault from the fault database, the fault must be resolved and a fault reset must be initiated (e.g. turn and release the Reset key switch on the BKM).



#### Attention

Make sure that the diagnostic message is understood and the fault is resolved before initiating a fault reset! Attempting a reset without checking the nature of the fault may lead to a recurring event.

---

## Principle of fault response



#### Attention

It is strongly recommended to repair faults even though a fault seems to have no effect on the system.

If not repaired immediately, faults may accumulate and -combined- create an unforeseen but expectable system response.

---

Each detected fault is reported by means of a diagnostic message, alarm markers and/or diagnostic markers.

If the nature of the fault requires the system to respond, Safety Manager will isolate the faulty component from the rest of the system.

At the same time the system acts on the effect of loosing the function of that component.

That action may be:

- none, a redundant component can cover for the lost function.
- none, loosing the function has no impact on safety.
- apply the fault reaction state to the affected IO.
- start the repair timer.
- halt the affected Control Processor.
- de-energize all non-redundant outputs via the watchdog
- de-energize all outputs via the watchdog.

Below explains these items in more detail.

## Redundancy

When available, the redundant component in the system will continue to perform that function. This means that, when redundancy is provided, the system remains available for the process.

## No impact on safety



### Attention:

When below faults occur, the system will report the anomaly but take no action by itself. However the system can be programmed to initiate action if needed.

---

The following examples show a number of faults that have no impact on safety:

- External power down.
- Loss of communication with a process control system.
- Failure of the Controller back-up battery.

## Fault reaction state

If Safety Manager detects a fault related to the IO, this may result in the IO to go to the fault reaction state.

The fault reaction state is a state used as response to faults arising related to IO.

The fault reaction state is user configurable on module level for hardware IO and on point level for communication IO. The following fault reaction states exist:

- High is a fault reaction state for digital inputs:  
Upon a detected fault the input is energized, or -in other words, the input goes high or becomes '1'.

- **Low** is a fault reaction state for digital inputs and digital outputs:  
Upon a detected fault the digital input or output is de-energized, or -in other words, the digital input or output goes low or becomes '0'.
- **Top Scale** is a fault reaction state for analog inputs:  
Upon a detected fault the input is set to the top scale of the range.
- **Bottom Scale** is a fault reaction state for analog inputs:  
Upon a detected fault the analog input is set to the bottom scale of the range.
- **Scan** is a fault reaction state for tested (analog or digital) inputs:  
Upon a detected fault the input or output continues to carry the processing value, even if this value may be incorrect.
- **Hold** is a fault reaction state for analog and digital inputs:  
Upon a detected fault the input freezes to the last known good value.
- **0 mA** is a fault reaction state for analog outputs:  
Upon a detected fault the analog output is de-energized.
- **Appl** is a fault reaction state for all outputs:  
Upon a detected fault the output remains active, the output value may be incorrect.
- **Preset** is a fault reaction state for numeric inputs located on a communication channel:  
Upon detected fault the numeric input is preset to a predefined value (not necessary being the startup value).
- **Freeze** is a fault reaction state for numeric inputs located on a communication channel:  
Upon a detected fault the input freezes to the last known good value.

Table 9 on page 76 shows the settings applicable to fault reaction for hardware IO.

**Table 9** Fault Reaction settings for hardware IO

Signal type		Fault Reaction settings
Digital Inputs	Tested	High/Low/Scan/Hold
	Not Tested	High/Low/Hold
Safe Digital Inputs with Line Monitoring		High/Low/Scan/Hold
Digital Outputs	Tested	Low/Appl
	Not Tested	Low/Appl
Tested Digital Outputs with Line Monitoring		Low/Appl
Tested Analog Inputs		Top Scale/Bottom Scale/Scan/Hold

**Table 9** Fault Reaction settings for hardware IO

Signal type		Fault Reaction settings
Analog Outputs*	Tested	0 mA/Appl
	Not Tested	0 mA/Appl

\* The setting Tested or Not Tested is determined by the properties of the analog output module.

Table 10 on page 77 shows the settings applicable to fault reaction for communication IO.

**Table 10** Fault Reaction settings for communication IO

Signal type	Fault Reaction settings
Digital Points (DI)	High/Low/Freeze
Numeric Points (BI)*	Preset/Freeze

\* the default preset value for numeric points is 0

## Repair timer

All configurations of Safety Manager are single fault tolerant towards faults that affect safety: By using a secondary means Safety Manager is always able to bring a process to safe state, regardless of the fault.

However, given some time, a second fault may occur. This second fault may then disable the secondary means that keeps the process in a safe state.

To prevent such a scenario to develop, the system starts a repair timer if a secondary means becomes vulnerable to faults. Once started, this configurable timer counts down until the fault is repaired. If the timer is allowed to reach zero, the Control Processor halts.

## Halt Control Processor

A Control Processor halts if:

- A fault is detected in one of its safety functions.  
For example: corrupted software, safety processors out of sync, watchdog fault
- The repair timer runs out.
- The Control Processor is disabled by its own watchdog,
- The Control Processor is disabled by the watchdog of the other Control Processor.

## Watchdog and redundancy

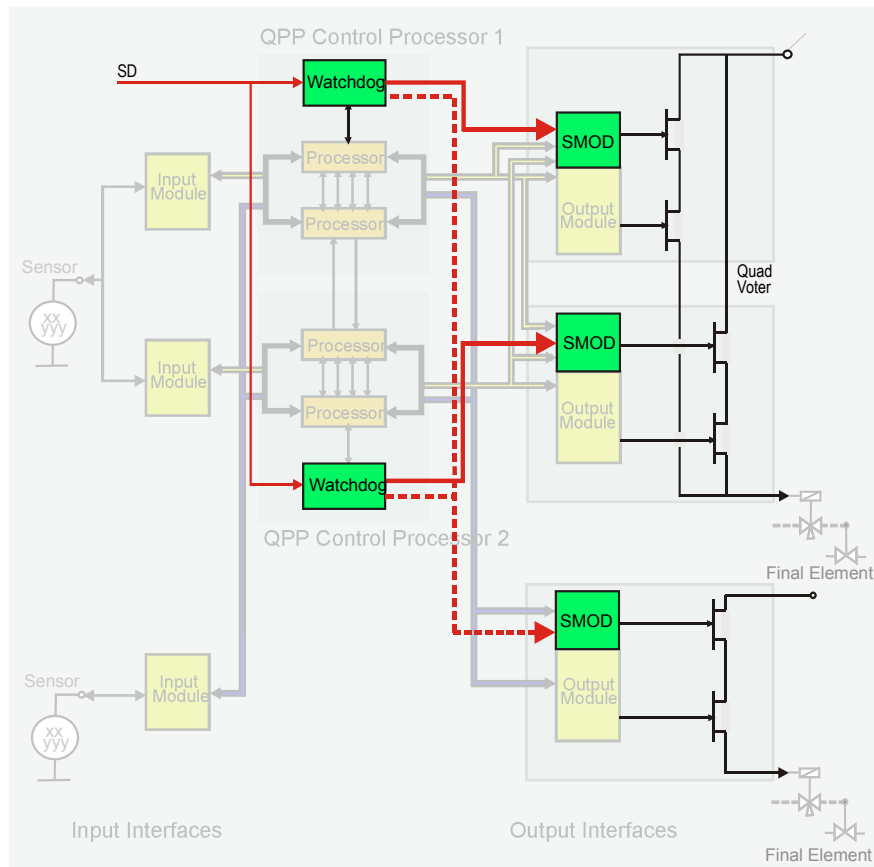
The availability of the system after responding to a fault depends on the available redundancy in the system and if -and how- the watchdog interfered.

As shown in Figure 25 on page 79 each Control Processor has a watchdog with two watchdog lines to independently enable/disable the (non-) redundant outputs.

If the watchdog interferes, this can be caused by:

- A fault in the Control Processor:  
This will halt the related CP and disable all output controls of that CP.
- A fault in the non-redundant outputs:  
This will cause the watchdogs of both Control Processors to disable the non-redundant outputs.
- A fault in one of the redundant outputs:  
This will cause the related watchdog to halt its CP and disable all outputs controlled by that CP.

**Figure 25** Each watchdog has 2 outputs



### Attention

It is strongly recommended to repair faults even though a fault seems to have no effect on the system. If not repaired immediately, faults may accumulate and -combined- create an unforeseen but expectable system response.

## Safety Manager alarm markers, registers and diagnostic inputs

Safety Manager has a number of inputs, generated by the system, that can be used in the application to indicate an alarm or a state:

- System markers and registers indicate the state of the system,
- Alarm markers indicate the occurrence of an abnormal system state,
- Diagnostic inputs indicate the health of the related IO channel or IO loop.

All three are discussed in this section.

Topic	See
System markers and registers	page 80
Alarm markers	page 81
Diagnostic inputs	page 83

### System markers and registers

System markers and system registers reflect the system state in the application.

#### System markers

The following system markers are available:

**Table 11** Safety Manager system markers

System marker	Description
FaultReset	Fault reset input
ForceEnable	Force enable
ClockSync	Clock synchronization input
CP1_Running	Control Processor 1 running
CP2_Running	Control Processor 2 running
ForceActive	IO forced
Flasher-0.5Hz	0.5 Hz flasher
Flasher-1Hz	1 Hz flasher
Flasher-2Hz	2 Hz flasher
Flasher-5Hz	5 Hz flasher



## System registers

The following system registers are available:

**Table 12** Safety Manager system registers

System register	Description
TempCP1	Temperature Control Processor 1
TempCP2	Temperature Control Processor 2
Second	Second
Minute	Minute
Hour	Hour
Day	Day
DayOfTheWeek	Day of the week
Month	Month
Year	Year

## Alarm markers

Safety Manager uses a number of alarm markers and alarm registers to indicate the occurrence of abnormal system state. Some markers are general markers, others are specific.

### Alarm markers

The following alarm markers are available:

**Table 13** Safety Manager alarm markers

Alarm marker	Description
TempHH_Alarm	Temperature high-high alarm
TempH_Alarm	Temperature high alarm
TempL_Alarm	Temperature low alarm
TempLL_Alarm	Temperature low-low alarm
ExtComFaultCC1	External communication fault in communication channel 1
ExtComFaultCC2	External communication fault in communication channel 2
ExtComFaultCC3	External communication fault in communication channel 3
ExtComFaultCC4	External communication fault in communication channel 4
ExtComFaultCC5	External communication fault in communication channel 5
ExtComFaultCC6	External communication fault in communication channel 6

**Table 13** Safety Manager alarm markers (*continued*)

Alarm marker	Description
ExtComFaultCC7	External communication fault in communication channel 7
ExtComFaultCC8	External communication fault in communication channel 8
ClockSrcFault1	Clock source 1 fault
ClockSrcFault2	Clock source 2 fault
ClockSrcFault3	Clock source 3 fault
SecSwitchOff	Secondary switch-off-Control Processor fault
CP_Fault	Control Processor fault
ControllerFault	Safety Manager controller fault
InputFault	Input channel fault
InputLoopFault	Input loop fault
InputCompare	Input compare fault
OutputFault	Output channel fault
OutputLoopFault	Output loop fault
OutputCompare	Output compare fault
RepairTimerStart_CP1	Repair timer started in CP1
RepairTimerStart_CP2	Repair timer started in CP2

### Remaining repair time

The following registers are available to indicate the remaining repair time:

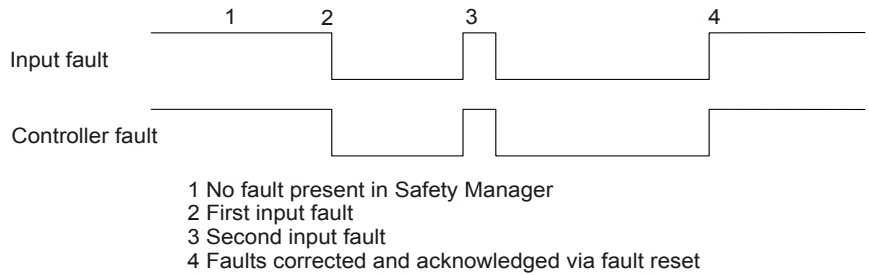
**Table 14** Safety Manager alarm registers

Repair timer registers	Description
Repair_CP1	Remaining repair time Control Processor 1
Repair_CP2	Remaining repair time Control Processor 2

### Alarm marker state

The normal state of a marker (no fault detected) is '1'. When the first fault is detected, the associated alarm marker changes to '0'. Any subsequent fault of the same type causes the alarm marker to pulse for one application program cycle (see Figure 26 on page 83).

**Figure 26** Input failure alarm marker function



## Diagnostic inputs

Diagnostic inputs are available for every Point allocated on a testable IO module.

There are basically two types of diagnostic inputs.

All diagnostic inputs can be used as a digital input in the functional logic diagrams to indicate the status of the IO.

### Diagnostic inputs related to channel status.

These indicate the diagnostic status of a specific IO channel allocated to a Safety Manager Safety Related IO module (see Table 15 on page 83).

**Table 15** Diagnostic inputs (channel status)

Type	IO Module
IO type I	SDI-1648, SDIL-1608
IO type O	SDO-0824, SDO-04110, SDO-0448, SDO-0424, SDOL-0424
IO type AI	SAI-0410, SAI-1620m
IO type AO	SAO-0220m
VM cab.c/s/17* (Voltage Monitoring)	SAI-1620m
EFM cab.c/s/ch** (Earth Fault Monitoring)	SDIL-1608

\* cab.c/s identifies the cabinet, chassis and slot number of the module. 17 is a dedicated channel for Voltage monitoring

\*\* cab.c/s/ch stands for cabinet, chassis, slot number and channel of the earth fault.

If the channel status is healthy, its diagnostic input is high. If a fault is detected in the channel, the diagnostic input goes low. The status of the diagnostic inputs does not depend on the safety relation of the channel.

#### Diagnostic inputs related to loop status.

These indicate the diagnostic status of a process loop in the field (see Table 16 on page 84).

**Table 16** Diagnostic inputs (loop status)

Type	IO Module
SensAI	SAI-0410, SAI-1620m transmitter status
LoopI	SDIL-1608 loop status
LoopO	SDOL-0424 loop status

When a Control Processor detects a loop fault, the system response sets the corresponding marker (SensAI, LoopI, LoopO) to faulty (value “low” or “0”).

## SM IO faults

Below topics provide an overview of detected IO faults and the Controller response to these faults.

Each topic is accompanied by a fault response table. The principle of these tables is explained in “Fault response tables” on page 85.

The following IO fault related topics can be distinguished:

Topic	See
Digital input faults	page 86
Analog input faults	page 87
Digital output faults	page 87
Analog output faults	page 89
IO compare errors and system response	page 90
Compare error detection and synchronization	page 92

### Fault response tables

Table 17 on page 85 explains the meaning of each column of the IO fault response tables.

**Table 17** Explanation of a “Controller response to faults” table

This row identifies the fault topic			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
This column identifies the type of fault. <i>Examples of a fault category are “loop faults” and “power”.</i>	This column identifies the core message of related diagnostic messages	Shows response of the CP with the faulty IO. <i>It indicates the field response for non-redundant IO</i>	Shows response of the CP without the faulty IO. <i>It indicates the field response for redundant IO</i>
		When both columns are merged the response of both CP’s is identical.	

### FR State

Some cells in the fault response tables state “*Apply FR state*”.

For an explanation of what this means see “Fault reaction state” on page 75.

**Tip**

- To see the Controller response towards non-redundant IO, check the “CP<sub>X</sub> (non-red)” column.
- To see the Controller response towards redundant IO, check the “CP<sub>Y</sub> (red)” column.

**Alarm markers**

All detected faults cause alarm markers to be set low or 0.

Depending on the fault, a single marker, or several markers are set. Some markers are general and are always set upon an IO fault.

For more information about alarm markers, see “Safety Manager alarm markers, registers and diagnostic inputs” on page 80.

**Digital input faults**

Table 18 on page 86 provides an overview of faults that can be detected in relation to digital inputs and the response to these faults.

**Table 18** Controller response to digital input faults

Digital input faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
digital input loop (line monitored)	lead breakage	apply FR state	apply FR state
	short circuit		
	earth fault		
loop power (default)	power output to sensors shorted	apply FR state	apply FR state
loop power (line monitored)	power output to sensors shorted	apply FR state	apply FR state
channel	channel faulty	apply FR state	none
module	module faulty	apply FR state	none
compare*	input compare error	apply FR state	apply FR state

\* See also “IO compare errors and system response” on page 90.

## Analog input faults

Table 19 on page 87 provides an overview of faults that can be detected in relation to analog inputs and the response to these faults.

**Table 19** Controller response to analog input faults

Analog input faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
analog input value	below low transmitter alarm level	apply FR state	apply FR state
	above high transmitter alarm level		
loop power	External voltage monitoring fault (SAI-1620m)	none	none
channel	channel faulty	apply FR state	none
module	module faulty	apply FR state	none
	Internal power down (SAI-1620m)		
compare*	input compare error	apply FR state	apply FR state

\* See also "IO compare errors and system response" on page 90.

## Digital output faults

Table 20 on page 87 provides an overview of faults that can be detected in relation to digital outputs and the response to these faults.

**Table 20** Controller response to digital output fault

Digital output faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
digital output loop (default)	Short circuit detected (single message)	De-energize shorted output(s).	
	Short circuit detected (multiple messages)		

**Table 20** Controller response to digital output fault (*continued*)

Digital output faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
digital output loop (line monitored)	current detected	apply FR state	
	open loop		
	Short circuit detected (single message)	De-energize shorted output(s).	
	Short circuit detected (multiple messages)		
loop power	external power down	none	
channel (default)	channel faulty	Apply FR state. • When FR state is low de-energize group & start repair timer	<b>IF</b> channel is non-redundant, CP <sub>Y</sub> responds like CP <sub>X</sub> . <b>ELSE</b> no response from CP <sub>Y</sub> .
	mismatch between expected and actual value	Apply FR state. • When FR state is low also de-energize group & start repair timer	<b>IF</b> channel is non-redundant, CP <sub>Y</sub> responds like CP <sub>X</sub> . <b>ELSE</b> no response from CP <sub>Y</sub> .
	channel cannot be switched off	Apply FR state. • When FR state is low also de-energize group & start repair timer	<b>IF</b> channel is non-redundant, CP <sub>Y</sub> responds like CP <sub>X</sub> . <b>ELSE</b> no response from CP <sub>Y</sub> .
channel (line monitored)	channel cannot be switched on	De-energize channel(s) that cannot be switched on.	



**Table 20** Controller response to digital output fault (*continued*)

Digital output faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
module	line monitoring circuit	Apply FR state. <ul style="list-style-type: none"> <li>When FR state is low also de-energize group &amp; start repair timer</li> </ul>	none none
	module faulty or all groups de-energized (non-redundant)	When FR state is appl: <ul style="list-style-type: none"> <li>Apply FR state to CP<sub>X</sub>,</li> <li>“none” response from CP<sub>Y</sub></li> </ul> When FR state is low: <ul style="list-style-type: none"> <li>Both CPs de-energize non-redundant IO watchdog line</li> </ul>	
	module faulty or all groups de-energized (redundant)	When FR state is appl: <ul style="list-style-type: none"> <li>Apply FR state to CP<sub>X</sub>,</li> <li>“none” response from CP<sub>Y</sub></li> </ul> When FR state is low: <ul style="list-style-type: none"> <li>halt CP<sub>X</sub></li> <li>“none” response from CP<sub>Y</sub></li> </ul>	
compare*	output compare error	apply FR state	

\* See also “IO compare errors and system response” on page 90.

## Analog output faults

Table 21 on page 89 provides an overview of faults that can be detected in relation to analog outputs and the response to these faults.

**Table 21** Controller response to Analog output faults

Analog output faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
power	external power down	none	

**Table 21** Controller response to Analog output faults (*continued*)

Analog output faults			
Related to	Diagnostic message reports	Controller fault response	
		CP <sub>X</sub> (non-red)	CP <sub>Y</sub> (red)
channel	mismatch between expected and actual value	Apply FR state on both CPs <ul style="list-style-type: none"> <li>When FR state is 0 mA also de-energize group &amp; start repair timer on both CPs</li> </ul>	
	channel faulty		
module	module faulty or all groups de-energized	Apply FR state on both CPs <ul style="list-style-type: none"> <li>When FR state is 0 mA also de-energize non-redundant IO watchdog line on both CPs</li> </ul>	
compare*	output compare error	Apply FR state.	

\* See also “IO compare errors and system response” on page 90.

## IO compare errors and system response



### Note

Because of the high level of self-testing and fault-handling by Safety Manager, the actual occurrence of a compare error is very unlikely.

For proper operation both Control Processors of a redundant system must have identical IO values at the beginning and at the end of each application cycle.

An IO compare error is generated as soon as the Controller detects a difference between the IO values of CP1 and CP2.

### Fault response table

This section uses fault response tables to explain the response towards faults.

Table 22 on page 91 explains the meaning of each column in the IO Compare error fault response table.

### FR State

Some cells in the fault response tables state “*Apply FR state*”.

For an explanation of what this means see “Fault reaction state” on page 75.

**Table 22** Explanation of a “Controller response to compare error” table

IO compare error			
Related to	redundancy	Occurs when detecting	Controller response
list type of IO	*	lists cause of the fault	identifies the response of the Controller

\* reports the configuration of IO (redundant or non-redundant).

### Different process values

Differences in process values may be caused by IO or synchronization faults. Such differences are usually solved before the application cycle starts.

- For more information regarding differences caused by IO faults see “Input compare errors” on page 92 and “SM IO faults” on page 85.
- For more information regarding differences caused by synchronization faults see “Input synchronization algorithm” on page 93.

### Controller response

The Controller responds towards IO compare errors by applying the fault reaction state to the faulty IO.



#### Note

A Controller does not automatically shut-down upon detection of IO compare error.

However, sometimes a shut-down is required to comply to local regulation. In such cases refer to “Shutdown at assertion of Safety Manager alarm markers” on page 110.

Table 23 on page 92 shows the relation between Input and output compare faults, alarm markers and Controller response.

**Table 23** Controller response to IO compare faults

IO compare error			
Related to	redundancy	Occurs when detecting	Controller response
digital inputs	N.A.	a persisting difference for more than 1 DTI	apply FR state
analog inputs	N.A.	a deviation of >2% for more than 1 DTI (SAI-1620m only).	
digital outputs	N.A.	a difference between outputs	
analog outputs	N.A.		

## Compare error detection and synchronization

### Input compare errors

Input compare error detection applies to all hardware inputs.

Differences in the input status read should be momentary. Persisting differences could be the result of detected hardware faults. In that case, the faulty input channel is reported in the diagnostics, and both Control Processors use the process value read from the healthy input channel.

A persisting difference in status of an input while no faults are detected at the accessory hardware channels leads to an input compare error.

### Output compare errors

An output compare error applies to all digital hardware.

In configurations with a redundant Controller, both Control Processors will continuously have an identical application status, resulting in identical process outputs.

An output compare error is detected if there is a difference between the Control Processors with respect to:

- the calculated application output values for digital outputs (DO) or communication outputs (DO, BO) to another Safety Manager.
- the actual application values sent to digital outputs (DO) or communication outputs (DO, BO) to another Safety Manager.

If outputs are no longer synchronized an Output Compare error is generated.

## Input synchronization algorithm

In configurations with a redundant Controller, the process inputs are scanned every application program cycle by both Control Processors.

Each Control Processor executes the application cycle independently of the other. It is therefore essential that they use identical values for the process inputs.

There is no problem if the process inputs are stable. However, if an input value changes when the Control Processors read the value, both Control Processors could read a different value. In such cases, an identical input value in the Controller is obtained via input synchronization.

If inputs are no longer synchronized, the signal value freezes to the last known synchronized state and a synchronization timer -equal to the configured Diagnostic Test Interval- is started. This state is maintained until:

- a synchronized state is obtained or
- the synchronization timer runs out.

If a synchronized state is not achieved within the configured Diagnostic Test Interval the fault reaction is activated and an Input Compare error is generated.

If a synchronized state is achieved within the configured Diagnostic Test Interval the synchronization timer is reset.

Synchronization algorithms are used for digital and analog inputs.

## Digital input synchronization

A digital input compare error is detected if the inputs of both Control Processors are stable but different (for example Control Processor 1 continuously '0', Control Processor 2 continuously '1'), for the duration of the configured Diagnostic Test Interval (DTI).

The input compare error detection algorithm puts the following demands on the dynamic nature of the digital process inputs:

1. If an input state changes, it must become stable again within the configured Diagnostic Test Interval.
2. The frequency of continuously changing inputs must be less than  $1/\text{DTI}$ .

## Analog input synchronization

For analog inputs, the synchronized value is the mean value of the input values. An input compare error is detected if the input values differ more than 2% of the full scale for the duration of the configured Diagnostic Test Interval.

The input compare error detection algorithm puts the following demands on the dynamic nature of the analog process inputs:

1. For inputs allocated on a redundant module (type SAI-0410 or SAI-1620m), the slope steepness must be less than 125 mA/s.
2. For inputs allocated on a non-redundant module (type SAI-1620m), the slope steepness must be less than 20 mA/s



**Caution**

Analog input compare errors may, for example, occur when calibrating smart transmitters using hand-held terminals. Refer to the *Troubleshooting and Maintenance Guide* for details on calibrating smart transmitters that are connected to Safety Manager analog inputs.

---

## SM Controller faults

Below topics provide an overview of detected Controller faults and the Controller response to these faults.

Each topic is accompanied by a fault response table. The principle of these tables is explained in “Fault response tables” on page 95.

The following fault topics can be distinguished:

Topic	See
QPP faults	page 96
USI faults	page 98
BKM faults	page 99
PSU faults	page 100
Communication faults	page 100

### Fault response tables

This chapter works with fault response tables to explain the response towards faults.

Table 24 on page 96 explains the meaning of each column in the various Controller fault response tables.



#### Tip

- The left column (CP<sub>X</sub>) identifies the response of the faulty Control Processor and can be seen as system response for a non-redundant system.
- The right column represents the system response when redundancy is provided.

**Table 24** Explanation of a “response to Controller faults” table

This row identifies the fault topic				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> ( faulty)	CP <sub>Y</sub> (not faulty)
identifies the type of fault.	See note*	lists the core message of related diagnostic messages.	lists the response of faulty CP	lists the response of other CP (if any!)
			When both columns are merged the response of both CP's is identical.	

\* This column identifies if the Controller response or set point can be configured by user setting.

### FR State

Some cells in the fault response tables state “*Apply FR state*”.

For an explanation of what this means see “Fault reaction state” on page 75.

### Alarm markers

All detected faults cause an alarm marker to be set low or 0.

Depending on the fault, a single marker, or several markers are set. Some markers are general and are always set upon a Controller fault.

For more information about alarm markers, see “Safety Manager alarm markers, registers and diagnostic inputs” on page 80.

### QPP faults

Table 25 on page 97 provides an overview of faults that the Controller detects related to the QPP and the response to these faults.



Table 25 Controller response to QPP faults

QPP faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> (faulty)	CP <sub>Y</sub> (not faulty)
temperature monitoring	set points	high alarm	run	run
		low alarm		
		high-high alarm	halt CP	run
		low-low alarm		
		1 sensor faulty and temp. and more than 3 degrees from shutdown limits	run	run
		1 sensor faulty and temp. and less than 3 degrees from shutdown limits	halt CP	run
Memory	no	QPP memory	halt CP	run
Execution	no	execution time out of range / failure	halt CP	run
		error on logical sheet	halt CP	halt CP
Watchdog	no	output shorted	halt CP	
		de-energized watchdog line for redundant outputs	halt CP	run
		de-energized watchdog line for non-redundant outputs	CP runs, but is not active on non-redundant outputs	run
Watchdog	no	faulty	halt CP	run
Bus drivers				
Internal link				
QPP module				
secondary switch-off	no	faulty	halt CP	run
repair timer	runtime	running	run	run
		expired	halt CP	run
software	no	corrupted	halt CP	run

**Table 25** Controller response to QPP faults

QPP faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> (faulty)	CP <sub>Y</sub> (not faulty)
intervention	no	QPP key switch to “IDLE” position	halt CP	run
		Spurious watchdog interrupt		
		safe state initiated		
		SD input de-energized	halt CP	halt CP
synchronization	no	QPP-0001	halt CP	run
		system software	halted CP does not start	run
		base timer	halt CP	run
		IO compare error	Both CPs apply FR state	
time sync	yes	source unavailable	Both CPs switch to other source	
internal communication	no		halt CP	run

## USI faults

Table 26 on page 99 provides an overview of detected faults in relation to the USI and the response to these faults.

A fault in the USI also means that the communication channels of that USI are down. For an overview of faults related to communication lines, see “Communication faults” on page 100.



### Attention

The column “Controller response” of Table 26 on page 99 applies only when no redundancy is provided in the communication. If redundancy is provided, the Controller response shall be “none”.

Table 26 Controller response to USI faults

USI faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> (faulty)	CP <sub>Y</sub> (not faulty)
Memory	yes	USI module	apply FR state to affected COM inputs	none
Execution				
communication		USI module		
module faulty		USI module		
synchronization		system software		
Memory		USI module		
software		corrupted		

## BKM faults

Table 27 on page 99 provides an overview of faults that can be detected in relation to the BKM and the response to these faults.

Table 27 Controller response to BKM faults

BKM faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> ( faulty)	CP <sub>Y</sub> (not faulty)
intervention during normal operation	no	reset key switch	Both CPs clear fault database, restart deactivated components	
		force key switch	Both CPs enable / disable forces	
intervention during OLM		reset key switch	start halted CP	halt running CP
key switch		reset key switch failure	run	
		force key switch failure	start repair timer	
module faulty	no	BKM module	run	run
battery	no	faulty / low	run	run
		lifetime expired		
		transport switch		

## PSU faults

Table 28 on page 100 provides an overview of faults that can be detected in relation to the PSU and the response to these faults.

**Table 28** Controller response to PSU faults

PSU faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			CP <sub>X</sub> (faulty)	CP <sub>Y</sub> (not faulty)
Voltage monitoring	no	spurious watchdog interrupt	halt CP	run
module faulty		PSU module		

## Communication faults



### Notes

- Please note that a fault in the communication lines may be caused by USI modules. For an overview of USI faults, see “USI faults” on page 98.
- Redundancy in communication channels can also be achieved with non-redundant systems by assigning two channels to a device. In this case the table heading “Controller fault response” no longer relates to CP<sub>X</sub> or CP<sub>Y</sub> but to Channel<sub>X</sub> or Channel<sub>Y</sub>.

Table 29 on page 100 provides an overview of faults that can be detected in relation to communication and the response to these faults.

**Table 29** Controller response to communication faults

Communication faults				
related to	user configurable	diagnostics report includes	Controller fault response	
			Channel <sub>X</sub>	Channel <sub>Y</sub>
Experion PKS, device communication	time-out	communication fault Channel <sub>X</sub> .	switch to Channel <sub>Y</sub>	continue, if configured
		communication fault Channel <sub>Y</sub> .	continue	switch to Channel <sub>X</sub>
		communication fault Channel <sub>X</sub> and Channel <sub>Y</sub> .	Both CPs apply fault reaction state to SM Controller inputs	
Safety Station	no	nothing*	none	none

- \* As it is quite common for portable Safety Stations to be (dis-)connected on a regular basis, no diagnostic report or alarm marker is linked to this event.

### **Communication time-out**

If no communication with the external device is established within a predefined time frame a communication time-out is generated.

A communication time-out always results in a communication failure.

Communication time-outs can be configured by the user. See “Rules of thumb with respect to safety and availability” on page 105.

If a device is connected to Safety Manager via a redundant communication link, the fault detection applies to each link separately resulting in single-fault tolerant communication.

---

## Calculation errors



### Caution

Safety Manager stops if a calculation error occurs.

---

Calculation errors may occur in the application program.

Calculation errors occur if:

- The calculated value of an analog output is outside the specified range.
- The square root of a negative number is taken.
- A divide-by-zero occurs.
- An overflow occurs during a calculation.
- The value for a counter is outside the specified range.

Calculation errors reflect an incorrect design of the application program for the intended function. Once a calculation error occurs for a specific process Point, a correct result of successive calculations based on this Point cannot be guaranteed.

Guidelines on how to avoid calculation errors in the Safety Manager application are presented below.

### Preventing calculation errors

Calculation errors can be prevented as follows:

- Overall process design.
- Inclusion of Safety Manager diagnostic data.
- Validation of signals in the Functional Logic Diagrams (FLDs).
- Exception handling during the actual calculation.

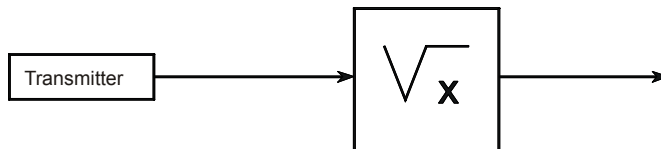
### Prevention by design

In line with good software engineering practice, as promoted by IEC 61508, calculation errors should be avoided by design. This means that an application should be designed in such a way that the operands of a symbol in the FLDs can never get an invalid value. The design approach starts with making sure that input values as obtained from the process remain within a predefined range. This approach ensures that the derived values are also valid for successive operations.

Sometimes, however, it cannot be guaranteed that an input value remains within a predefined range which is valid for all functions. For example, a signal derived

from a reverse-acting, non-linear 4-20 mA transmitter which has been configured for a zero top scale in the application domain could become negative if the transmitter fails and delivers a signal beyond 20 mA. If the signal is then linearized through a square-root function, a system stop occurs (square root of negative number).

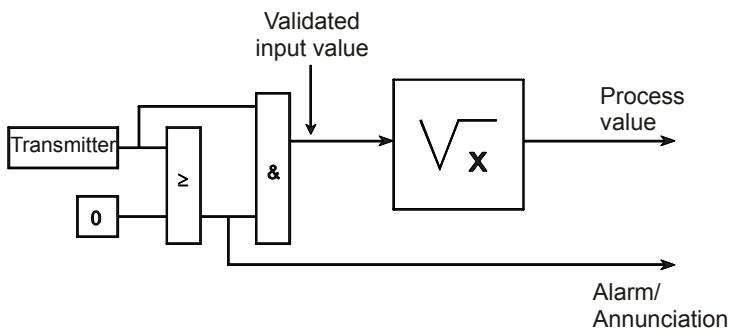
**Figure 27** Intended square-root function



### Preventive measures

If a valid input value cannot be guaranteed, preventive measures must be built into the design. A comparison function can be used as an indicator that the transmitter value has left its normal operational band and that the calculation should not be done. The alarm signal is used to implement a corrective action and to indicate the exception to the operator (see Figure 28 on page 103).

**Figure 28** Square-root function with validated input value



If diagnostics are not available (e.g. for 0-20 mA transmitters), it is necessary to implement range checking in the application. The result of the range check is again used for the implementation of corrective actions.



### Tip

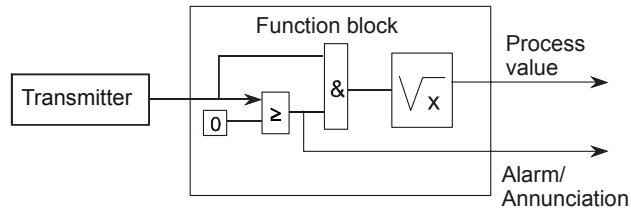
Range checking is also useful to define the boundaries of analog outputs 0(4)-20mA, thus preventing a system shutdown due to driving values that exceed the boundaries.

An important advantage of input validation is that it can be implemented for input values of which the validity cannot be guaranteed. Furthermore, the invalid input can be exactly identified. This allows the implementation of effective correction strategies of only the affected part of the process.

### Common function block

A last option is to create a common function block, e.g. square root. The function block validates the operand(s) and only performs the intended function if the operands are valid. Otherwise a predefined value is returned. An additional function block output should be provided which indicates if the calculation result is valid or not. This output signal can be used for the implementation of corrective actions in the application (see Figure 29 on page 104).

**Figure 29** Square-root function with validity check in function block





# Rules of thumb with respect to safety and availability

The philosophy behind the concept of fault reaction is to grant the design engineer the choice of customizing the system's fault reaction towards the safety and availability demands of the process.

Rules of thumb with respect to safety and availability settings can be divided in the following topics:

Topic	See
IO settings	page 105
System settings	page 106

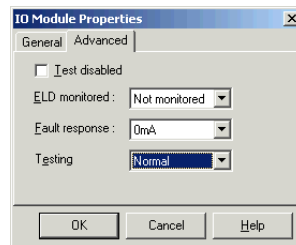
## IO settings

IO settings determine the response of Safety Manager towards detected faults related to the IO.

### Analog output property settings

Figure 30 on page 105 shows the module properties of an analog output module. The properties of this module has the check box **Test disabled** which can be checked.

Figure 30 Properties of an analog output module



Checking this box prevents the system from testing and generating undesired warnings. On the other hand will this also prevent the system from generating safety related warnings.



### Warning

When checking the **Test disabled** check box the analog output module may not be used as part of a safety loop.

### Advised fault reaction settings

- For normally energized safety related applications, like ESD applications, the advised predefined safe state is de-energized or ‘Low’.
- For normally de-energized safety related applications, like FGS applications, the advised predefined safe state for inputs is energized or ‘High’ / ‘Top Scale’.
- For all other applications a preferred safe state cannot be determined beforehand; the user can choose between scanning (‘Scan’) and freeze last known value (‘Hold/Freeze’).

### Advised safety related settings

Figure 31 on page 106 provides an example of point properties. Each point has the **Safety related** pull down menu with the options **No** and **Yes**. (Initially this field is undefined.)

For hardwired IO these options have no effect on the system response. The selection made in this pull down menu is for documentation purposes only.

Figure 31 Point detail

The screenshot shows a 'Point detail' configuration window. The 'Details' section includes fields for Type (set to 'DI'), Tag number ('Digital\_Input'), Description, Status, Unit, Sub unit, SIL, Safety related (set to 'Undefined'), FLD Number (0), Location, Force Enable, and Write Enable. Below this is the 'Communication allocation' section, which contains a table with columns for Allocation, Logical connection, and PLC address. The 'Hardware allocation' section features dropdown menus for Size (1), Chassis, Slot, and Channel. To the right is the 'Field Input Device' section with a Type dropdown (Undefined). Navigation buttons are located at the bottom right of the window.

## System settings

System settings determine the response of Safety Manager towards detected faults not directly related to the IO.

## **Advised SIL level**

The Safety Integrity Level (SIL) field shows the highest SIL level Safety Manager is used for.

This variable has no impact on the system response towards safety related faults since the system response towards these is always based on SIL 3.

## **Advised repair timer settings**

A repair timer is a configurable count-down timer triggered upon detection of a fault that minimizes the safety availability of the system.

The repair timer settings determine the time period that faulty Control Processors and their outputs allowed to continue without being halted. The default setting for a repair timer is 200 hours.

Extending the repair time increases the risk of a second fault arising and affecting the safety of the process; this is to be avoided whenever possible.

When in doubt, consult your Safety Matter Expert at Honeywell.



### **Caution**

Make sure that a running repair timer is recognized and can be responded to, before the repair timer expires.

---

## **Advised DTI settings**

Safety Manager uses the DTI to detect and respond to faults.

To detect all safety related hardware and software faults in a Safety Instrumented System (SIS), a fixed Diagnostic Test Interval must be determined.

The Diagnostic Test Interval depends on:

1. the Process Safety Time,
2. the demand mode of operation and
3. the amount of hardware and software to be tested.

The DTI for Safety Manager is never shorter than 1 second.

Within the Safety Manager, the default Diagnostic Test Interval is set at typically 3 seconds. This setting needs to be verified for each process.

Changing the DTI setting affects the application cycle time.

- Reducing the DTI will:
  - Cause the application cycles to become longer
  - Cause the system to respond faster to detected faults
- Increasing the DTI will:

- Cause the application cycles to become faster
- Cause the system to respond slower to detected faults

# Using Safety Manager alarm markers and diagnostic inputs

# 8

Safety Manager alarm markers and diagnostic inputs can be used within the functional logic diagrams (FLDs) to monitor and respond to changing system states, alarms and diagnostics.

This is illustrated by the following three examples.

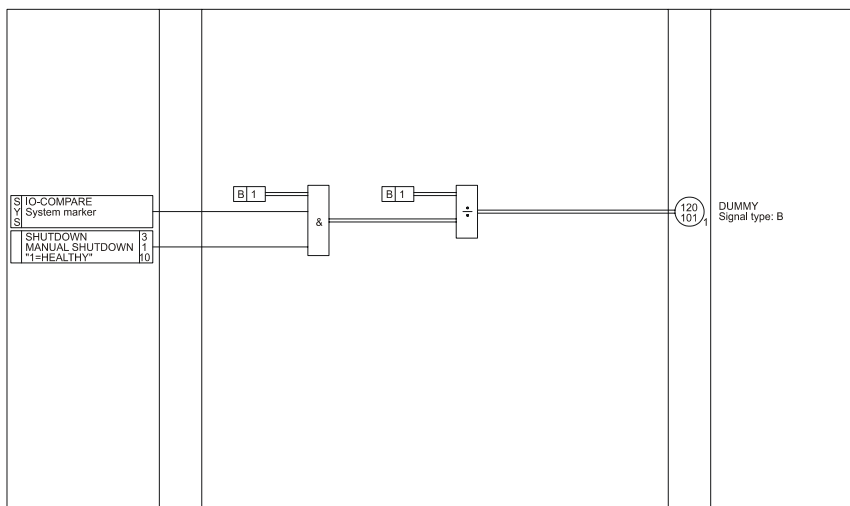
Example	See
<b>Shutdown at assertion of Safety Manager alarm markers</b>  This example shows how to program a shutdown in case of assertion of Safety Manager alarm markers. This kind of programming could be used if the system is intended to run in SIL3 without operator surveillance.	page 110
<b>Unit shutdown</b>  This example shows how diagnostic inputs of type IO-TYPE O can be used to realize independent safeguarding of process units including unit shutdown in case of defects.	page 111
<b>Diagnostic status exchange with DCS</b>  This example discusses the functional logic which can be used to report the status of alarm markers and diagnostic inputs to a distributed control system (DCS).	page 115

## Shutdown at assertion of Safety Manager alarm markers

If it is not sufficient to initiate an alarm when Safety Manager detects a fault and immediate system response is required, the Safety Manager alarm markers can be used to shut down the system via the application.

Figure 32 on page 110 shows an example of how to shut down the system in case of an IO compare error. An additional manual shutdown input is provided with which the operator can initiate a shutdown by hand.

**Figure 32** Diagram to shut down system in case of output compare error



If an IO compare error is detected or a manual shutdown is initiated, a divide-by-zero is forced and Safety Manager shuts down. Other alarm markers can be used in a similar way.



### Note

A manual shutdown can also be realized via the shutdown (SD) input of the SM Controller. In this way, a tested solid-state hard wired connection can be used, which allows the secondary means of de-energization of all outputs to be de-activated. This unique feature allows an ESD push button chain to be connected to Safety Manager which can then be used to initiate an emergency shutdown (ESD), fully independent of the Control Processor.

# Unit shutdown

## Process units

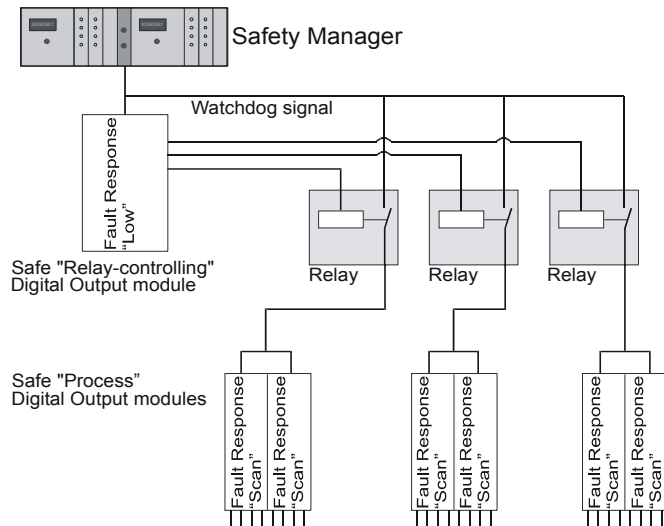
If a process can be divided into independent process units, the overall process availability can be increased by a separate shutdown of the units within Safety Manager. In this way, whenever a fault is detected in the hardware of a process unit, only the affected unit needs to be shut down, while the other parts of the process remain unaffected.

## Configuration of unit shutdown (watchdog grouping)

This subsection covers the required configuration, application programming and wiring to achieve shutdown per process unit.

Figure 33 on page 111 shows a standard wiring diagram for unit shutdown of three separate process units.

**Figure 33** Wiring diagram for unit shutdown



For each process unit, a relay is used to connect the watchdog signal of the unit output to the process Safety Manager watchdog. The relays are controlled via outputs of Safety Manager: the unit shutdown outputs. In normal operation, all relays are activated. If a fault is detected in a process unit, the corresponding relay is deactivated, which results in a shutdown of the relevant unit.

The unit relays must meet the requirements of DIN VDE 0116, part 8.7.4.5 and 8.7.4.6 of October 1989, i.e.:

1. Mechanical reliability  $> 3 * 10^6$  switches.
2. Contacts protected (for example fuses, series resistors, etc.) at  $0.6 * \text{nominal contact current}$ .
3. Electrical reliability  $> 2.5 * 10^5$  switches.



**Tip**

The relay output FTA TSRO-0824 complies to these requirements.

---

### Unit shutdown outputs

The unit shutdown outputs must:

- Be allocated on safe modules (such as a SDO-0824 or SDOL-0424 module)
- Have their '*fault reaction state*' set to 'low'.  
This guarantees that Safety Manager directs the process to its safe state if a fault occurs which affects this output.
- Have set the '*power-up status*' of the unit shutdown output to 'ON'.  
This allows a correct start-up of Safety Manager with activated unit relays.

For optimal availability it is recommended that unit shutdown outputs are allocated to redundant output modules.

### Process outputs (safety related)

The process outputs must be allocated to a Safety Manager output module of the type:

- SDO-0824      Safety-related digital output module  
(24 Vdc, 0.55 A, 8 channels)
- SAO-0220m    Safety-related analog output module  
(0(4)-20 mA, 2 channels)
- SDO-04110    Safety-related digital output module  
(110 Vdc, 0.32 A, 4 channels)
- SDO-0448      Safety-related digital output module  
(48 Vdc, 0.75 A, 4 channels)
- SDO-0424      Safety-related digital output module  
(24 Vdc, 2 A, 4 channels)
- SDOL-0424    Safety-related loop-monitored digital output module  
(24 Vdc, 1 A, 4 channels)



To allow the programming of the response via the application, the fault reaction of these outputs must be set to 'Appl'. This disables the automatic response of Safety Manager in case a fault occurs at safety-related output modules.

## Application programming

To realize unit shutdown in the functional logic diagrams, all diagnostic inputs related to output modules of each process unit are connected to an AND gate.

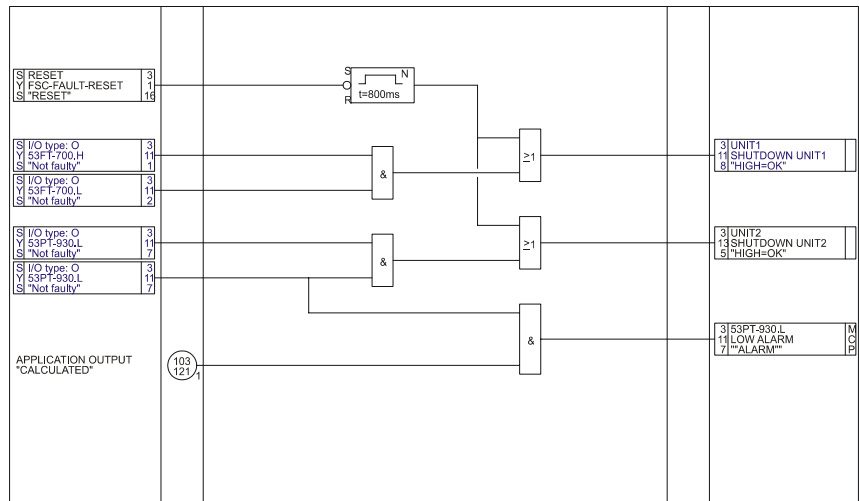
For a listing of diagnostic inputs related to output modules see “Diagnostic inputs” on page 83.

Figure 34 on page 113 shows how the output signal of the AND gate is connected to the unit shutdown.

As long as all diagnostic inputs are “healthy”, they are high, the unit shutdown output is high and the unit relay is activated (relay contact closed).

If a diagnostic input of an output channel in the unit becomes “unhealthy”, the corresponding unit shutdown output becomes low and the unit relay is deactivated (relay contact open).

**Figure 34** Functional logic diagram of unit shutdown



A defective output channel can be switched-off in accordance with the normal Safety Manager response for safety-related signals. To switch off a defective output channel, the calculated application output and the channel diagnostic input must be supplied to the output channel via an AND gate.

The Safety Manager ‘*FaultReset*’ alarm marker is connected to all unit shutdown outputs via an OR gate. When an error is detected and repaired in a unit, the unit may be restarted using the ‘*FaultReset*’ alarm marker.

The minimum and maximum time the unit output is enabled by the ‘*FaultReset*’ is limited to ensure that the ‘*FaultReset*’ is detected by the output. The pulse length (typically set at 800 ms) may not exceed the Diagnostic Test Interval.

# Diagnostic status exchange with DCS

## Distributed control systems (DCS)

Safety Manager alarm markers and the diagnostic inputs can be transferred to distributed control systems (DCSs), for example to generate an operator alarm or to initiate a corrective action within the DCS.

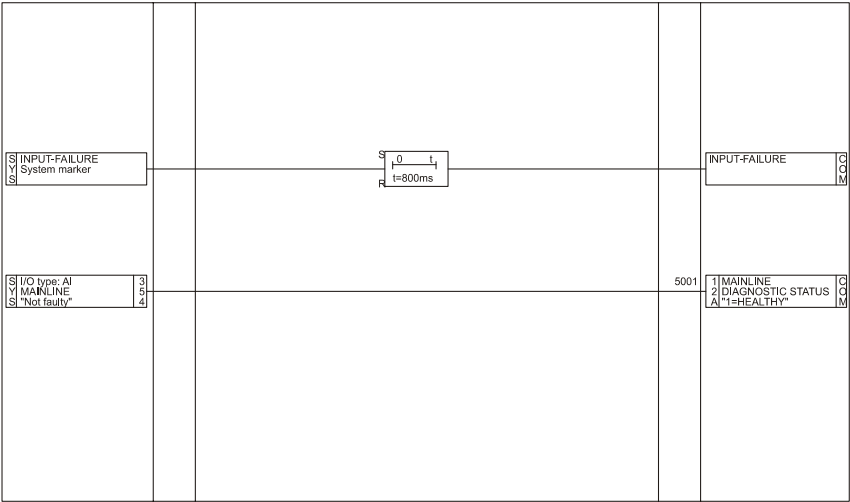


**Note**

Experion PKS can also access diagnostics through dedicated interfaces. See *Overview Guide* for details.

Figure 35 on page 115 shows the functional logic diagram to report the occurrence of an input fault ('InputFault' alarm marker) and the use of a diagnostic input (IO type AI) to report the status of an analog input channel to a DCS system.

**Figure 35** Safety Manager system information to DCS



The status of the Points is transferred to the DCS via outputs with location 'COM', which are allocated to the communication channel to the DCS.

### **Behavior of alarm markers**

The behavior of the alarm markers is quasi-static. Normally, if no fault is present, the value of the markers is high. If a fault is detected, the corresponding alarm marker becomes low. On subsequent faults the alarm marker becomes high during one application program cycle of Safety Manager (for example 300 ms) and then low again (see “Safety Manager alarm markers, registers and diagnostic inputs” on page 80).

If the scan cycle of the DCS lasts longer than the Safety Manager application cycle, it is possible that any subsequent faults are not detected by the DCS. The Safety Manager alarm marker is therefore connected to the output of the DCS via a delayed off timer. Thus, a pulse on the alarm marker is extended to the configured timer value. To ensure detection by the DCS, the timer value must be larger than the DCS scan time.

### **Behavior of diagnostic inputs**

The behavior of the diagnostic inputs is static. Normally, an IO channel is healthy and the value of the corresponding diagnostic input is high. If the IO channel becomes faulty, the diagnostic input becomes low. It remains low until the fault is repaired and a fault reset has been given. The diagnostic input can therefore be connected directly to the output to the DCS.

# Fire and gas application example

# 9

Following topics are described in this section:

Topic	See
Introduction	page 118
General system and Fire and Gas alarms	page 119
Input loops	page 122
Loop status	page 123
Output loops	page 125
Monitoring for alarm status	page 133
Monitoring for failure status	page 136
Inhibit function	page 138

---

## Introduction

This section describes an application for a Fire & Gas (F&G) application which is designed according to the requirements of EN-54 part 2 and NFPA 72, with the INHIBIT options installed. The basic Fire and Gas application is based on the basic Fire and Gas function described in Cause & Effect diagrams (for details see the Fire and Gas Application manual). The actual basic F&G application for Safety Manager is stored as BFGA\_1 revision 0.

Safety Manager does not support alphanumeric displays, so this option of EN-54 part 2 and NFPA 72 is not shown here. Visualization of alarms, faults, inhibits etc. will be arranged by means of lamps or leds on a mimic panel (common alarms, faults, etc.) and graphical displays on Experion PKS (common and detailed alarms, faults, etc.). On Experion PKS all alarms, faults, inhibits, status and warning signals will be collected listed in alarm list screens and will be stored for historian functions.

The figures in this chapter are FLDs taken from the basic F&G application BFGA\_1. Where applicable, references to the EN-54 part 2 or NFPA 72 standard are shown in italics in square brackets. The status of the installation that is monitored and the status of Safety Manager must be uniquely displayed [*EN-54 part 2, 7.2*] [*NFPA72, 3.8.7*]. In the complete example this is accomplished by the use of hardwired digital IO signals, which can drive LEDs, or lamps on the mimic panel for the common alarm, fault and inhibit signals.

Detailed alarm signals as well as common alarm, fault and inhibit signals will also be displayed on Experion PKS. These signals are transferred to these systems via the communication networks such as the Safety Manager-Safety Manager communication link or the dedicated Experion Ethernet network. [*EN-54 part 2, 7.9*] [*NFPA72, 1.5.4.4*]. Failure of the communication link must be alarmed [*EN-54 part 2, 8.2.5.b*].

Please note that the sheet references to safety functions in the functional logic diagrams must point to a higher FLD number, which means that they are used in the same application cycle to get the best possible response time. This response time of automatic fire detectors resulting in the required outputs is 3 seconds [*EN-54 part 2, 7.7.2*] [*NFPA72, 1.5.4.1.2, 1.5.4.2.2 & 1.5.4.3.3*].

---

## General system and Fire and Gas alarms

The system alarm FLD 2000 (Figure 36 on page 120) covers the status indication that the Safety Manager F&G control system is powered on and switched on, the indication for an earth leakage alarm [EN-54 part 2, 8.2.4.c] and the indication for a PSU or power failure [EN-54 part 2, 8.2.4.b, 8.2.4.d].

FLD 2002 (Figure 37 on page 120) contains the common failure alarm that is set in case of a failure of a component in the Fire & Gas detection system, including failures in the F&G detectors. A fault results in activation of the (yellow) General fault indication lamp [EN-54 part 2, 8.2.1.a, 8.5.a] and activation of the General Fault buzzer [EN-54 part 2, 8.2.1.c, 8.5.b] [NFPA72, 1.5.7.4] on the mimic panel. The buzzer can be silenced by means of a reset buzzer [EN-54 part 2, 8.6.1] switch on the panel. A new fault alarm activates the buzzer again [EN-54 part 2, 8.6.3].

FLD 2004 (Figure 38 on page 121) contains the common Fire/Gas alarm that is set in case of detection of fire or gas by the Fire & Gas detection system. An alarm results in activation of the (red) General Fire/Gas alarm indication lamp [EN-54 part 2, 7.2.a] and activation of the General Fire/Gas alarm buzzer [EN-54 part 2, 7.2.c] on the mimic panel. The buzzer can be silenced by means of a reset buzzer [EN-54 part 2, 7.4.1] [NFPA72, 1.5.7.2] switch on the panel. A new alarm activates the buzzer again [EN-54 part 2, 7.4.3].

The failures in the F&G detectors are handled in other FLDs, in this example see FLD 530 (Figure 39 on page 121) of a smoke detector input loop [EN-54 part 2, 8.1.1]. Inside function block FB2411 alarm and fault signals are generated for this detector and used in the logic. Smoke detectors have an automatic latching function. Detectors in alarm state have to be reset by switching off detector device [EN-54 part 2, 7.6.1]. This reset function is included in the function block.

Figure 36 FLD2000 system alarms

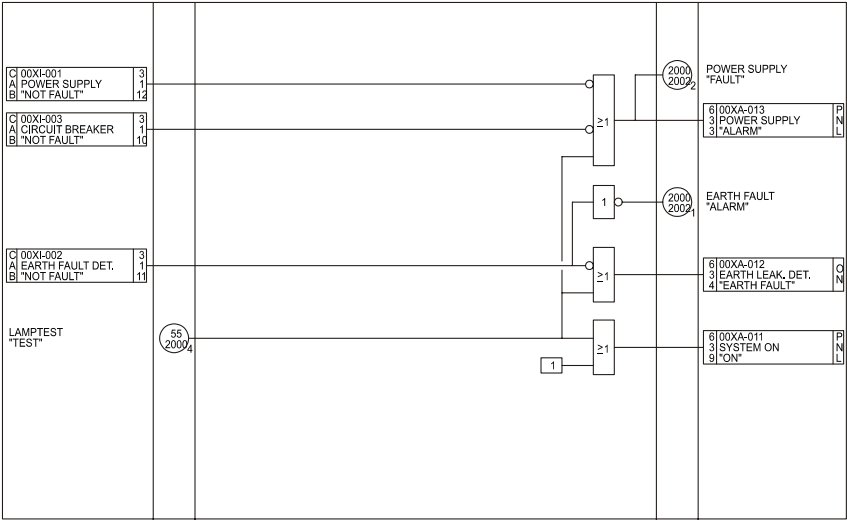
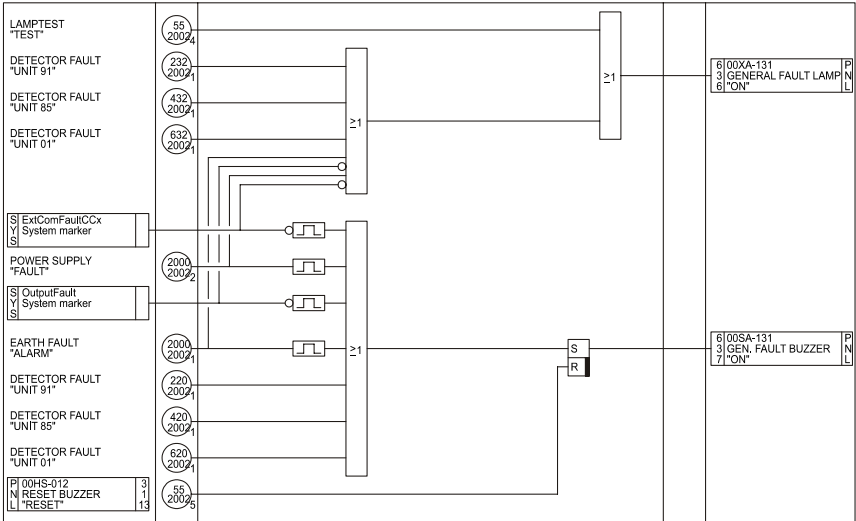
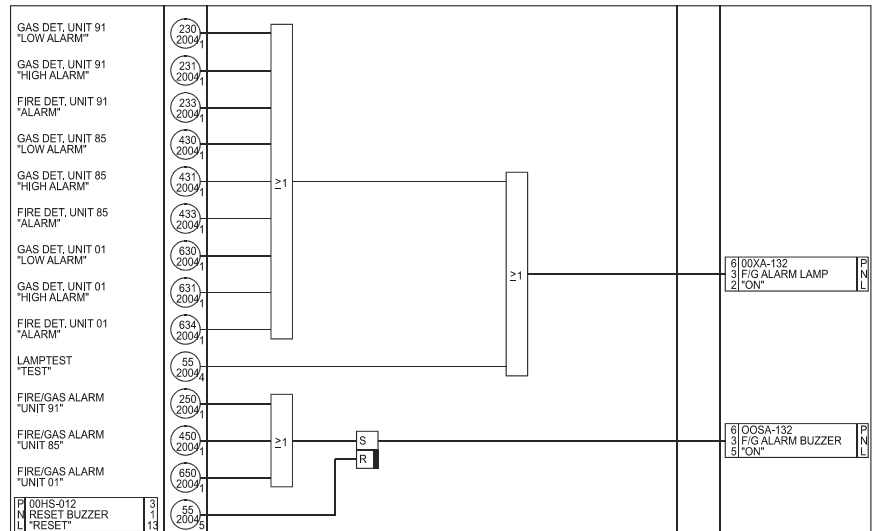


Figure 37 FLD2002 general fault alarm

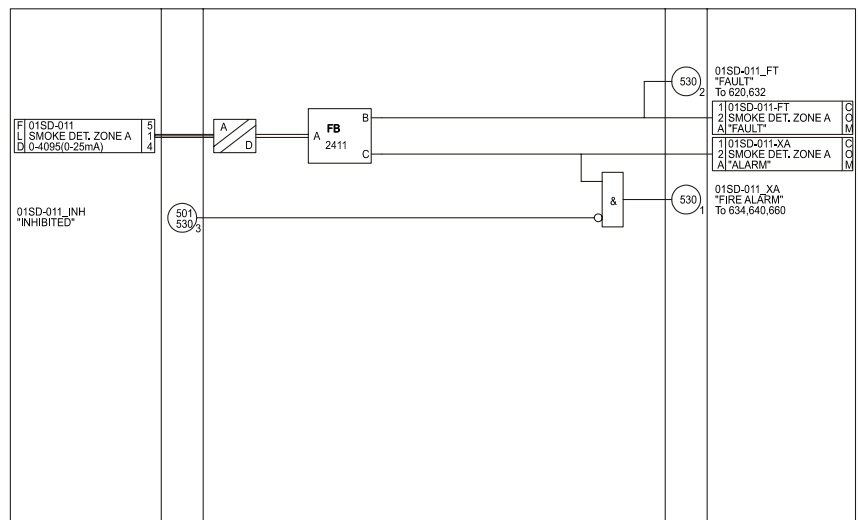




**Figure 38** FLD2004 general fire/gas alarm



**Figure 39** FLD530 smoke detector input loop

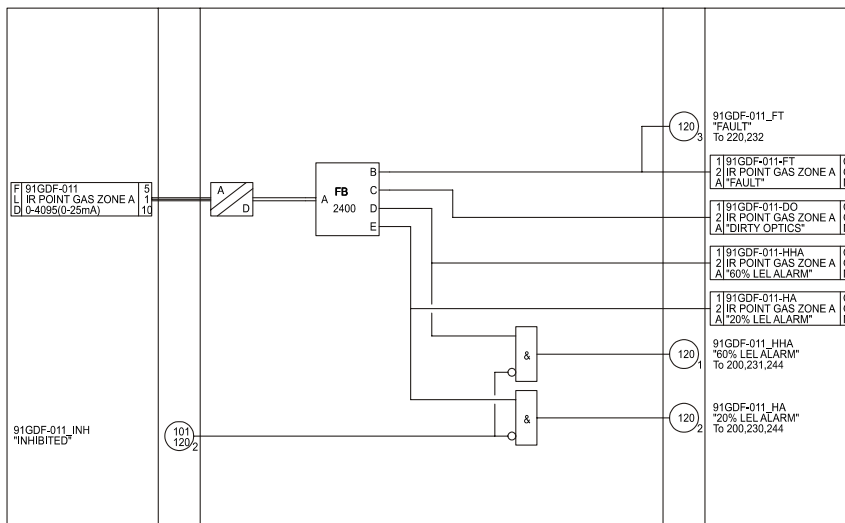


## Input loops

The basic Fire and Gas application has a number of Fire & Gas detector input loops (see FLD 530 (Figure 39 on page 121) and FLD 120 (Figure 40 on page 122)). The Fire & Gas detectors are connected to analog input modules. The output of the detectors can be a digital contact with loop-monitoring or an analog input signal. The function blocks 2400, 2401, 2402, 2403, 2404, 2405, 2411, 2412 and 2413, handle all functions for an input loop [EN-54 part 2, 7.1.2, 7.1.5]. These functions are:

- Setting of alarm and fault levels [EN-54 part 2, 7.1.2].
- Loop status (open loop, short-circuit) as determined by Safety Manager [EN-54 part 2, 8.2.4] [NFP472, 1.5.8.1].
- Inhibit for the input loop [EN-54 part 2, 8.1.2].

Figure 40 FLD120 gas detector input loop



# Loop status

The loop status (operational status, failure status and inhibited status) is indicated on TPS or Experion displays with an indication per status [EN-54 part 2, 7.2.b, 7.3.1, 8.2.1.b] [NFPA72, 1.5.7.1.1]. All states are also transferred to other FLDs via sheet transfers to generate the common status indication and to drive the audible indications (horn) [EN-54 part 2, 7.8]. [NFPA72, 1.5.7.2]

Individual fault, alarm and inhibit signals are also grouped per area or zone for the indication on TPS or Experion displays and on the mimic panel [NFPA72, 1.5.7.1.2]. See FLD 230 common low level alarm (Figure 41 on page 123) and FLD 232 common detector fault (Figure 42 on page 124).

**Figure 41** FLD230 common low level alarm Area 1

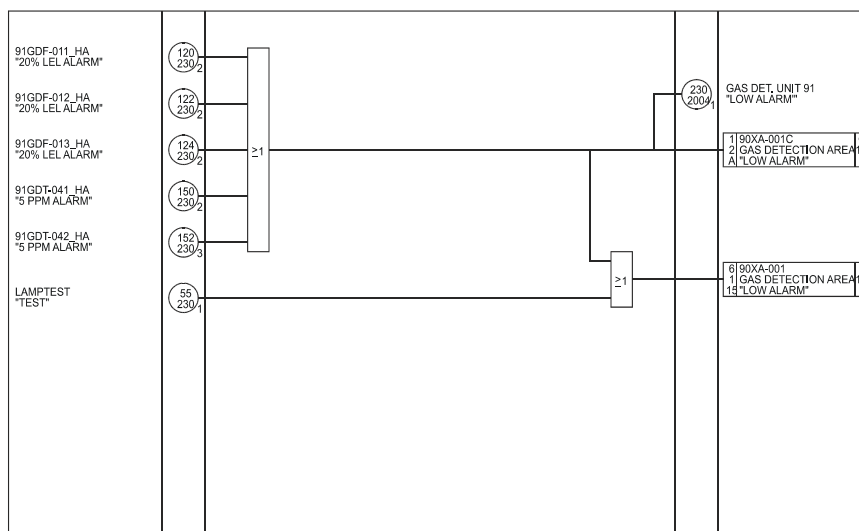
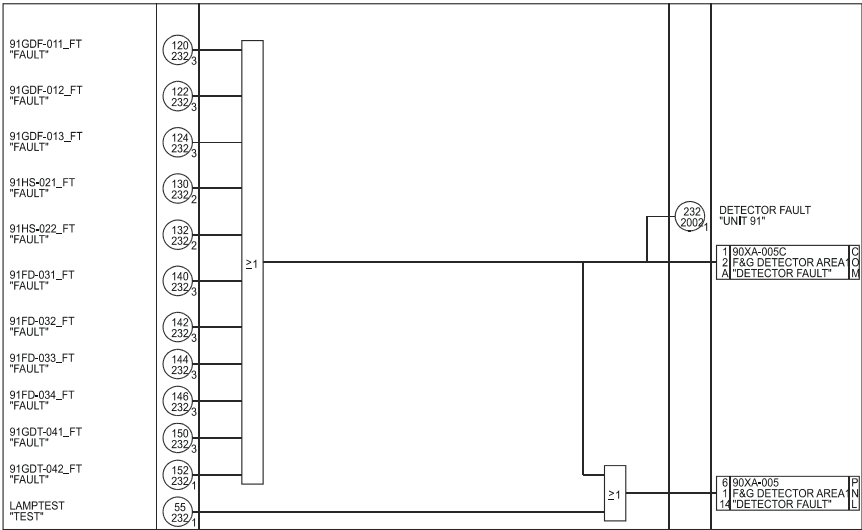


Figure 42 FLD232 common F&G detector fault Area 1



---

# Output loops

The basic Fire and Gas application has a number of output loops for the required safety actions and annunciation.

The various different output loops are described in detail below.

## Sounders and beacons

One of the main tasks of a F&G safety system is to alert people of potential hazards and initiate the required evacuation of buildings and areas [*NFPA72, 3.2*].

The main notification appliances are beacons, sounders and bells. An example of these sounders and beacons can be found on FLD 240 (Figure 43 on page 126).

These sounders and beacons shall be assigned and installed for each zone or area [*NFPA72, 1.5.7.3*].

These output signals are normally of the “energize-for-action” type. This means that a Safe reaction of the F&G safety system does not result in activation of these external alarming devices.

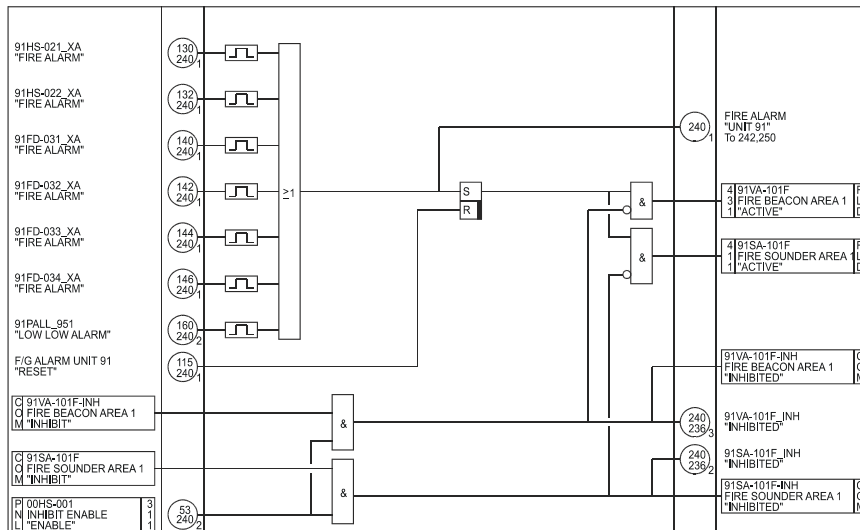
The loop shall be monitored for short circuit as a minimum [*NFPA72, 1.5.8.4*], while other possible faults, e.g. open loop or ground fault, shall not influence other output loops [*NFPA72, 1.5.8.3*].

It is advised to connect the notification appliances to line-monitored digital output modules, type SDOL-04xx. These modules provide full line-monitoring detection of short circuit as well as open loop.

Devices that have a very high power consumption cannot be connected to SDOL-04xx modules. In those cases the installation of an external switching device close to the notification appliance is advised. A SDOL-04xx module can monitor the loop to this external switching device.

Power can also be supplied by means of a Safe relay contact that switches the required power to the external device. For these solutions a short test-interval time is advised to assure regular testing and proper functioning of the non monitored parts of these output loops.

Figure 43 FLD240 sounders and beacons



## Deluge valve

The deluge valves of fire suppression systems are often directly controlled by the F&G safety system.

An example of the connection of such a deluge valve can be found on FLD 290 (Figure 44 on page 127).

These output signals are normally of the “energize-for-action” type. This means that a Safe reaction of the F&G safety system does not result in opening of the valve.

The deluge valves shall be connected to line-monitored digital output modules, type SDOL-04xx. These modules provide full line-monitoring of short circuit as well as open loop.

The status signals of the deluge valve (see FLD 162, Figure 45 on page 127) and related fire suppression system (see FLD 160, Figure 46 on page 128) are normally monitored and sent to the control system [NFPA72, 3.8.6.3].

Figure 44 FLD290 deluge valve

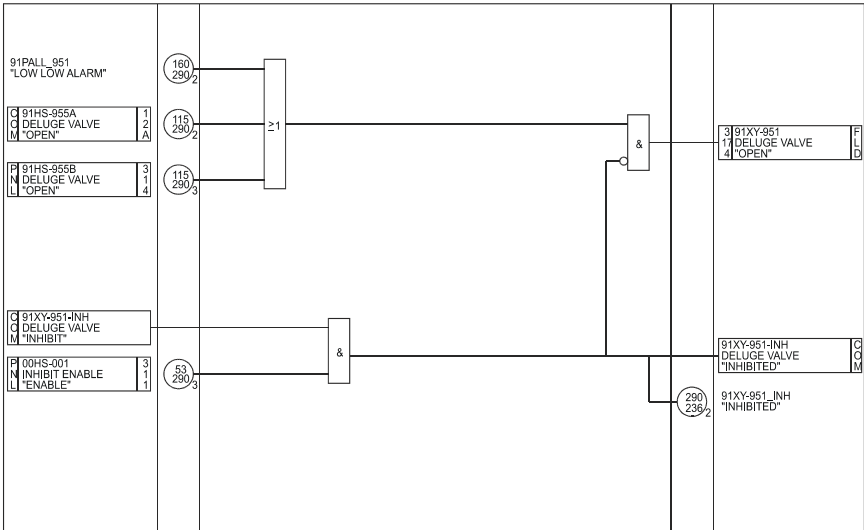


Figure 45 FLD162 status signals deluge valve

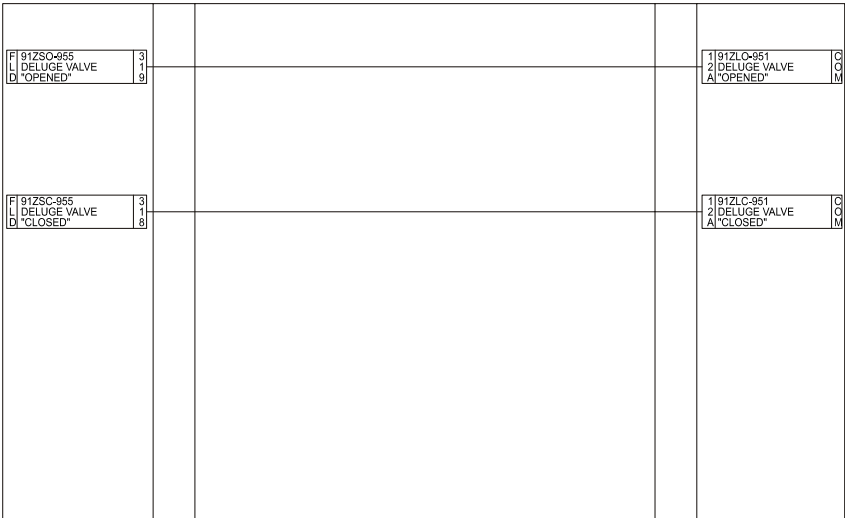
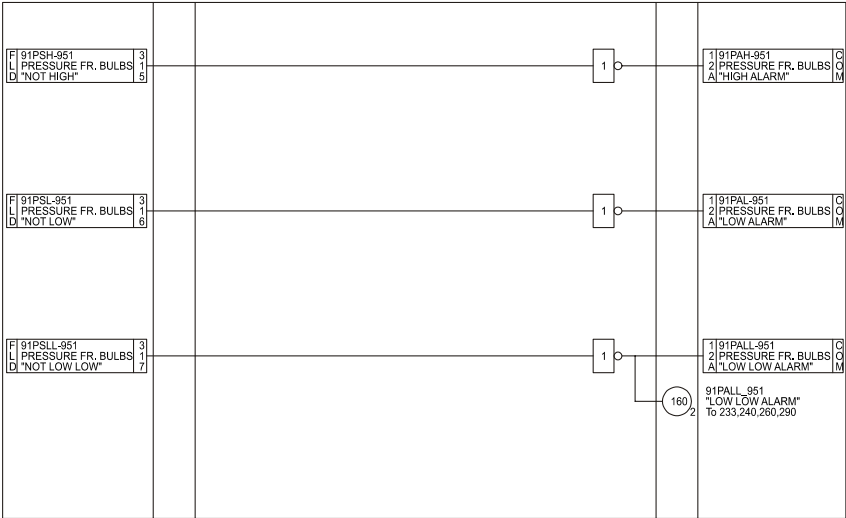


Figure 46 FLD160 status signals fire suppression system



### Firewater pumps

The firewater pumps for the fire suppression systems are often directly controlled by the F&G safety system.

An example of the connection of firewater pumps can be found on FLD 260 (Figure 47 on page 129).

The firewater pumps are started by fire or gas detection of the F&G safety system or by manual activation on the mimic panel.

The status of the firewater pumps is monitored by the F&G safety system [NFA72, 3.8.9], to check the actual state. It checks the required running state because firewater pumps can also be started manually or by other systems, see FLD 262 (Figure 48 on page 129).

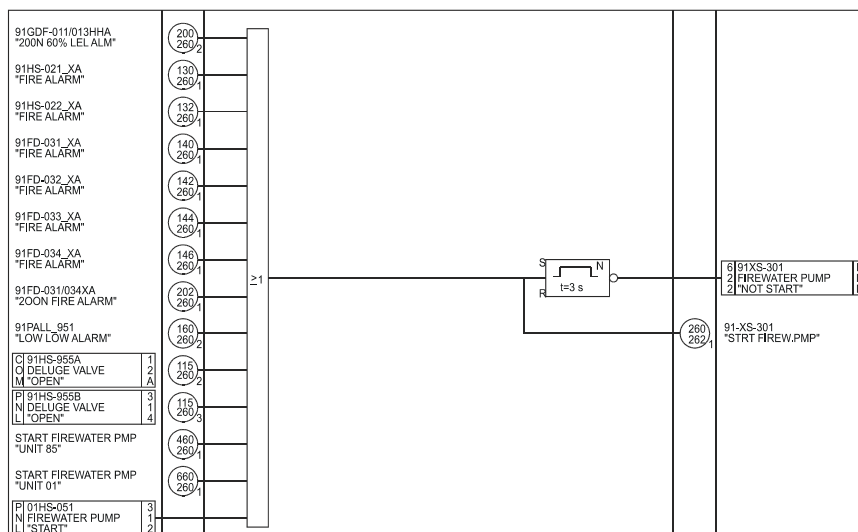
The start signal of the firewater pump of the F&G safety system is normally a “de-energize-to-start” type. This means that the Safe state of the F&G safety system starts the firewater pumps. The firewater pumps do not normally activate the fire suppression systems but bring these systems to the required pressure.

In the case that the start of the firewater pumps do initiate the activation of the fire suppression systems, the start signal is of the “energize-to-start” type so that the Safe states of the F&G safety system do not directly lead to activation of the fire suppression systems. These signals are normally line-monitored.

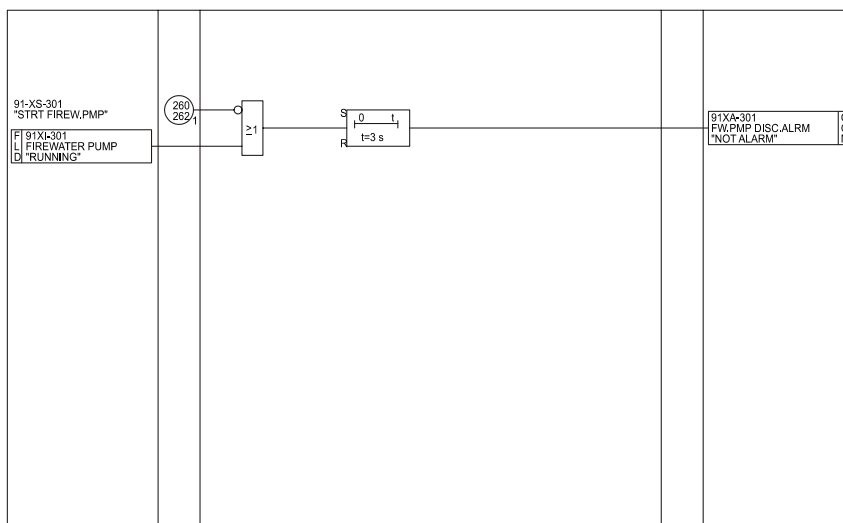


The start signals are normally pulsed and routed via dedicated motor control systems. These systems shall comply with the required standards [NFPA72, 3.8.9.1].

**Figure 47** FLD260 start firewater pump(s)



**Figure 48** FLD262 discrepancy alarm firewater pump



PA/GA system

The F&G safety system can sent an alarm signal to the PA/GA system.

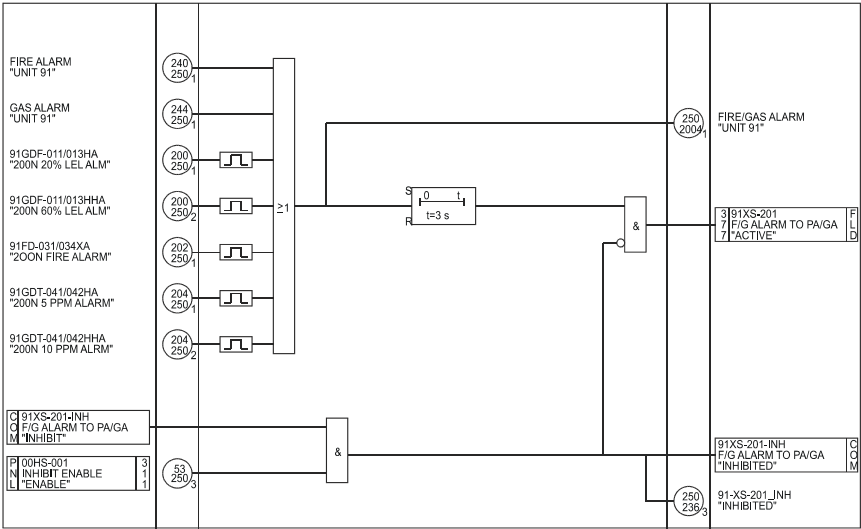
An example of the connection of PA/GA system can be found on FLD 250 (Figure 49 on page 130).

The F&G safety system sends the alarm signal to the PA/GA system on a confirmed fire or gas detection.

The alarm signal to the PA/GA system of the F&G safety system is normally a “energize-to-start” type. This means that the Safe state of the F&G safety system does not lead to an F&G alarm to the PA/GA system. The signals in the basic F&G application are usually pulsed which depends on the actual requirements by the PA/GA system.

The PA/GA system shall comply with the required standards [NFPA72, 3.12].

Figure 49 FLD250 alarm signal to PA/GA



HVAC system

The climate in the rooms protected by the F&G safety systems is normally controlled by HVAC systems.

A HVAC system has to act in the case of the fire or gas detection. A part of these control actions are taken by the HVAC system. The F&G safety system transmits a hardwired fire alarm signal to the HVAC system in the case of a hazard detection [NFPA72 3.9.3.4]. This signal to the HVAC system of the F&G safety system is normally a “energize-to-act” type, so the Safe state of the F&G safety

system does not lead to actions by the HVAC system. See for example FLD 680 (Figure 50 on page 131).

The HVAC system normally also includes special fire dampers. These dampers are normally directly controlled by the F&G safety system, see for example FLD 690 (Figure 51 on page 132).

These signals are of the “energize-to-open” type. This means that the Safe reaction of the F&G safety system leads to closure of the fire dampers.

**Figure 50** FLD680 HVAC trip signal

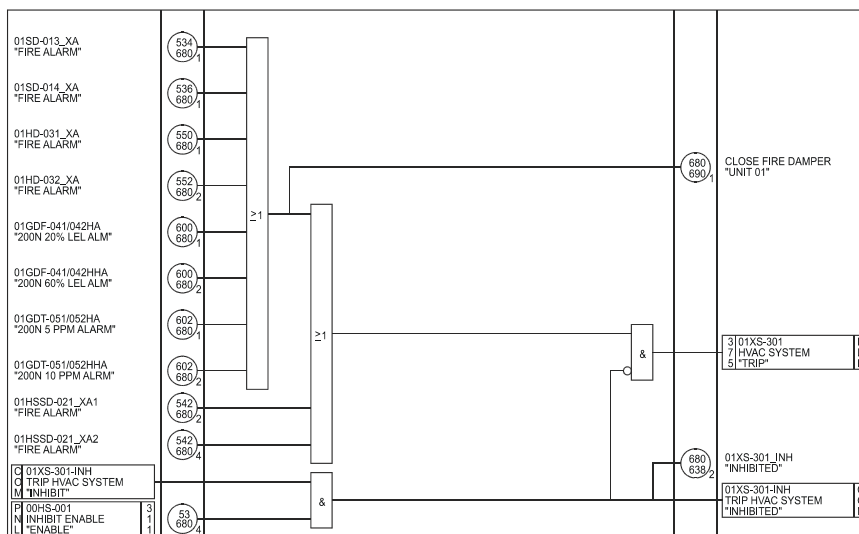
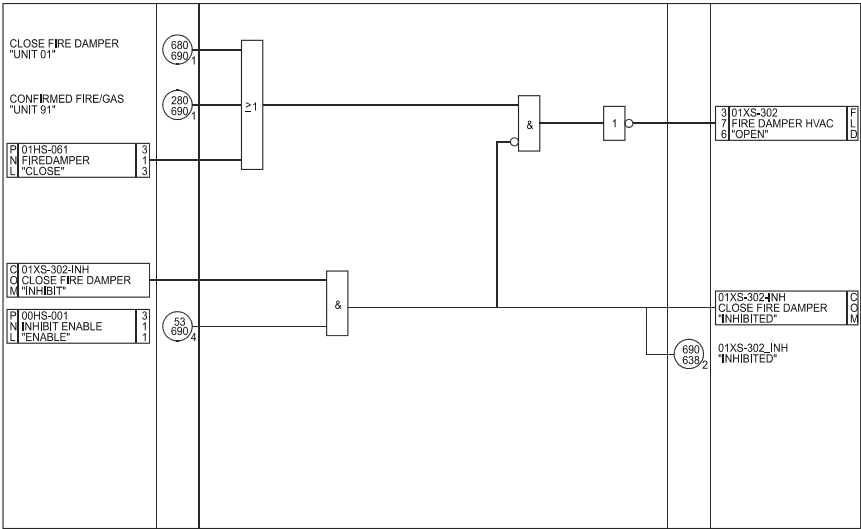


Figure 51 FLD690 close fire damper signals



---

## Monitoring for alarm status

The input loops are monitored for alarms. If an alarm status occurs, an audible alarm (horn) must also be activated [EN-54 part 2, 7.1.4].

The first type of audible alarm is located on the mimic panel and operator consoles. For this purpose the alarms of all F&G detectors are grouped (see FLD 250, Figure 52 on page 134) to activate common F&G audible and visual alarm in FLD 2004 (Figure 53 on page 134).

In this example these alarms activate an alarm signal to an external PA/GA system as well [EN-54 part 2, 7.9].

The output signal to the PA/GA system can be inhibited as required by the applicable standards [EN-54 part 2, 9.4.1.c].

The second type of audible alarms is located inside the buildings and the detection zones to alert people in the affected zones for potential hazards. For this purpose the alarms of all F&G detectors are grouped per area or zone (see Figure 54 on page 135) to activate the common F&G audible alarms in the affected areas. Normally these audible alarms are combined with visual alarm devices such as flash beacons. [EN-54 part 2, 7.8]. The output signal to the sounders and beacons can be inhibited as required by the applicable standards [EN-54 part 2, 9.4.2.a].

The visual alarm remains active as long as an alarm is active [NFPA72, 1.5.7.1], the audible alarm can be silenced by means of a reset signal [EN-54 part 2, 7.8.a]. For compliance with NFPA 72, this switch shall be of the key type [NFPA72, 1.5.4.8]. A new F&G alarm activates the horn again [EN-54 part 2, 7.4.3].

Figure 52 FLD250 grouping of alarm signals

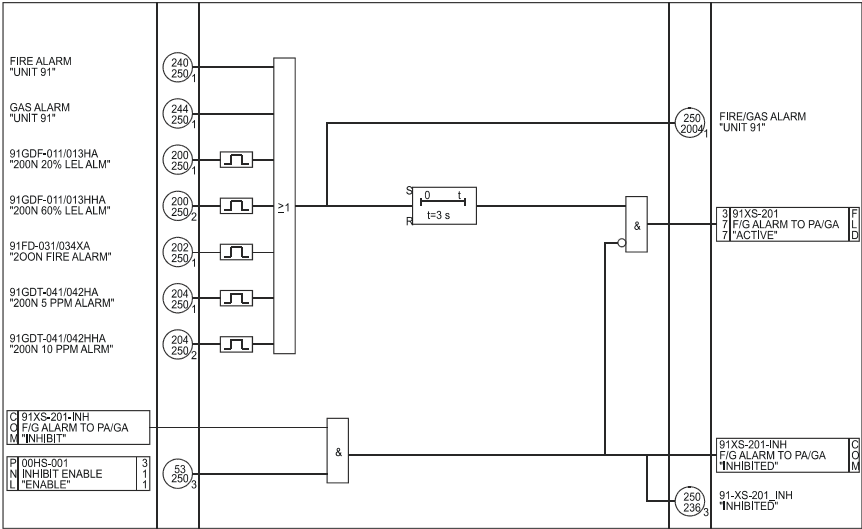


Figure 53 FLD2004 Fire and Gas alarm lamp and buzzer on mimic panel

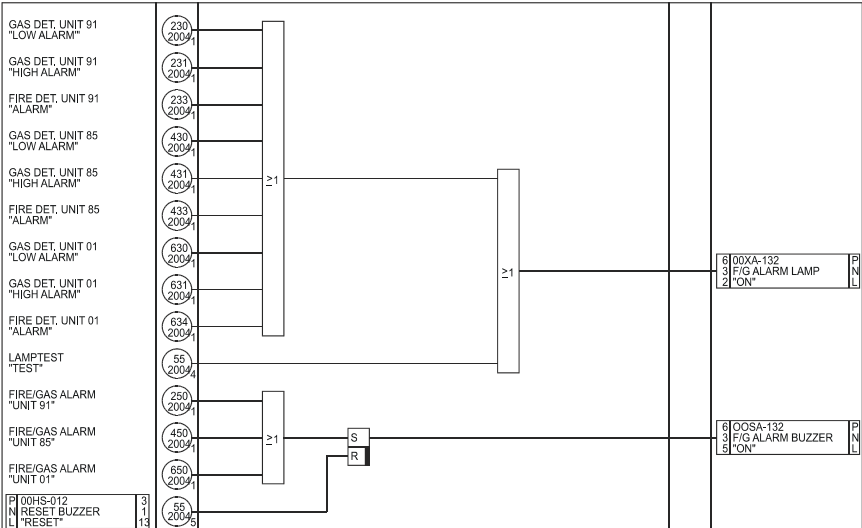
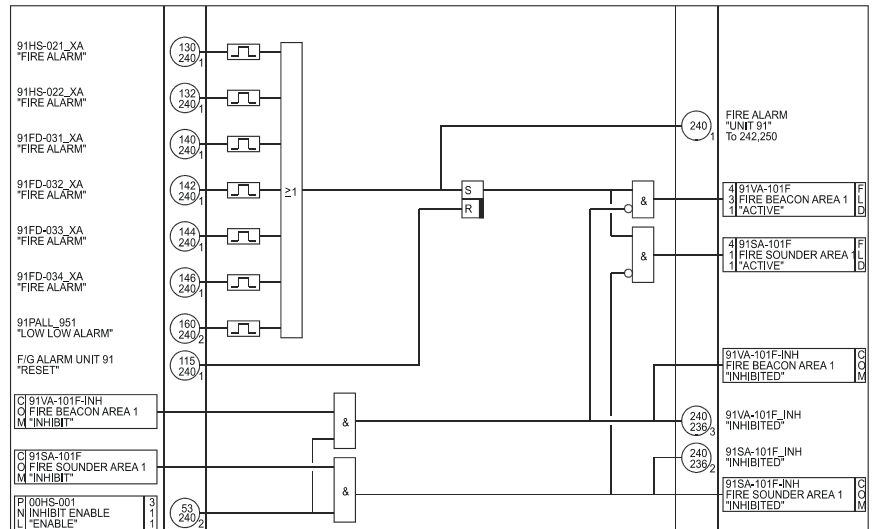


Figure 54 FLD240 audible and visual alarm signals

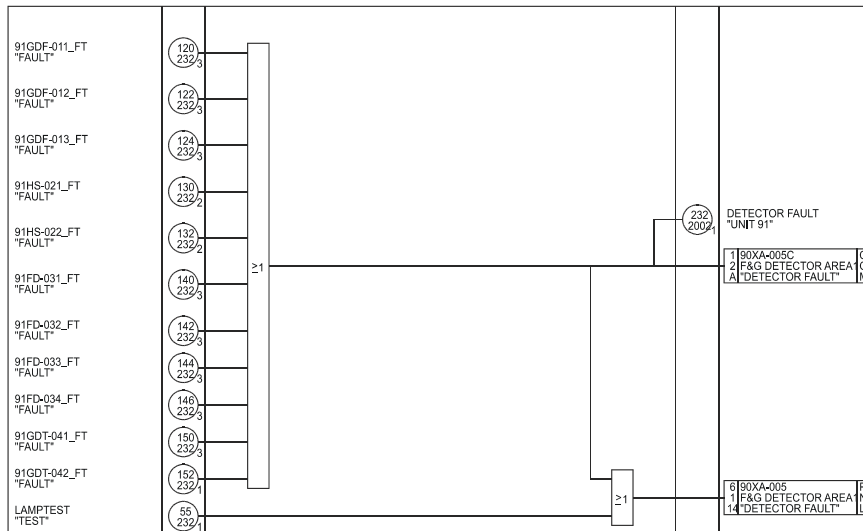


## Monitoring for failure status

All components of the Fire & Gas system, including the input loops and output loops, are monitored for failures [EN-54 part 2, 8.2.4, 8.2.5.a] [NFPA72, 1.5.8.1]. If a failure occurs, an audible alarm (horn) must be activated which has a different tone than the Fire & Gas audible alarm [NFPA72, 1.5.4.6.1, 1.5.4.7 & 3.7.2].

This audible alarm is located on the mimic panel and operator consoles [NFPA72, 1.5.4.6.2]. For this purpose the faults of all F&G detectors are grouped (see FLD 232, Figure 55 on page 136) to activate a common General fault audible and visual alarm in FLD 2002 (Figure 56 on page 137).

Figure 55 FLD232 grouping of detector fault signals



The other faults collected in FLD 2002 (Figure 56 on page 137) to generate general fault alarm are:

- ‘*OutputFault*’ which indicates if an output module or F&G output loop is faulty [NFPA72, 1.5.8.4].
- Power supply failures which indicate that a power supply or circuit breaker fails. [NFPA72, 1.5.8.6.1]
- Earth leakage failure which indicates that an earth fault has been detected.

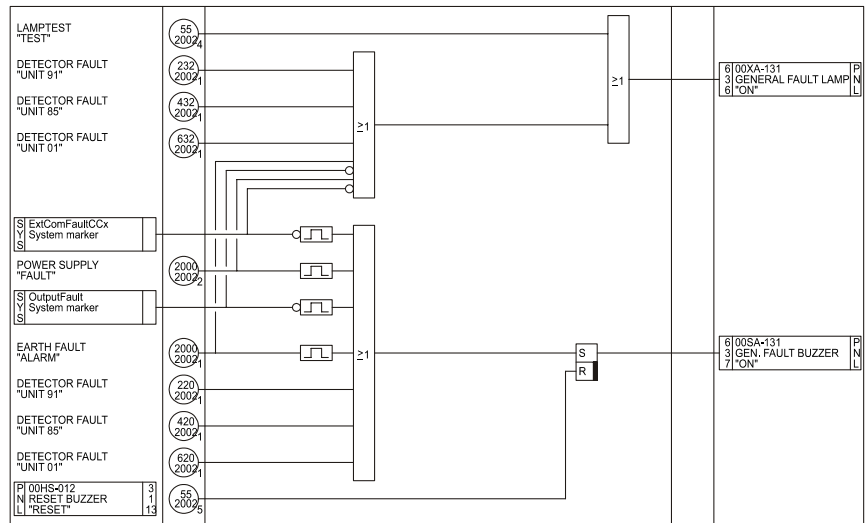


- ‘*ExtComFaultCCX*’ which indicates that a communication error is detected in communication channel X (select one of 8 available channels) [EN-54 part 2, 8.9].

Depending on the application, other internal failures of Safety Manager can also be covered by the common failure alarm. If more than one failure group is used in a Fire & Gas detection system, logic as shown in FLD 2002 (Figure 56 on page 137) is required for each failure group.

The visual alarm remains active as long as a fault is active [NFPA 72, 1.5.4.6.3], the audible alarm can be silenced by means of a reset signal [EN-54 part 2, 8.6.1]. For compliance with NFPA 72, this switch shall be of the key operated type [NFPA 72, 1.5.4.6.4]. A new fault will activate the horn again [EN-54 part 2, 8.6.3].

**Figure 56** FLD2002 general fault alarm lamp and buzzer on mimic panel

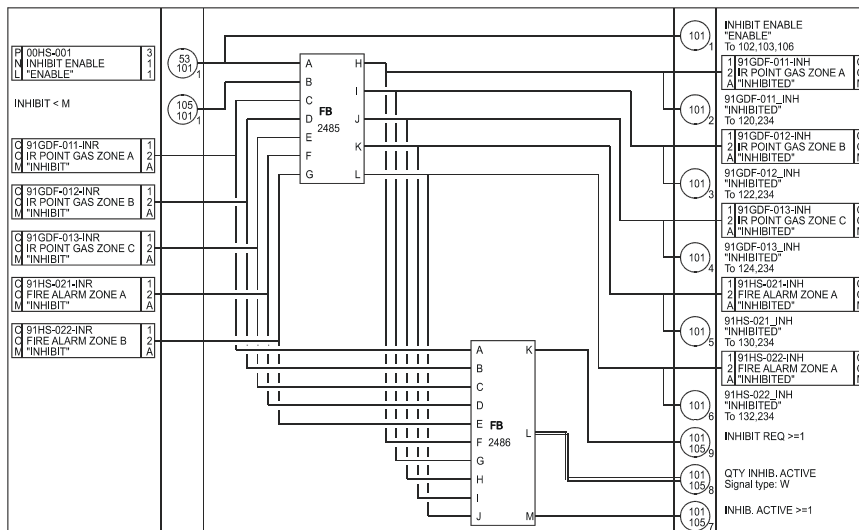


## Inhibit function

During operation it may be required that a detector device needs to be inhibited for a certain period to avoid nuisance alarms during that period [EN-54 part 29.4.a]. An inhibit can be required during the replacement of the detector device or because of other external activities (e.g. welding activities in the neighborhood of a smoke detector).

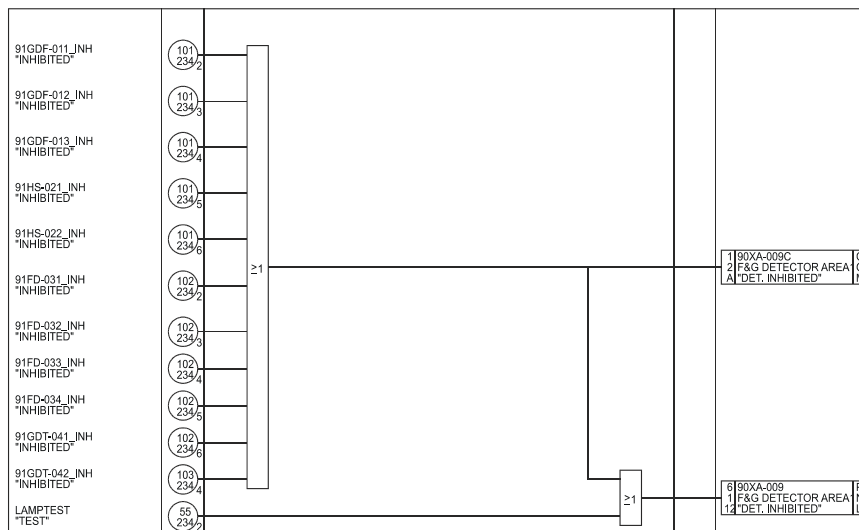
Inhibition of a detector device is only allowed under certain conditions. The inhibition has to be enabled by means of a hardwired ENABLE switch [EN-54 part 2, 9.1.2] on the mimic panel and Safety Manager checks that only a certain amount of inhibits (M) are active within a predefined group. The inhibit request of a certain detector device is made by the operator on the operator console by means of a soft key switch. The inhibit request signal is transferred to Safety Manager via the serial link. Safety Manager checks if the conditions are met (ENABLE switch on, amount of active inhibits < M). In case the inhibit request is granted, the inhibit indication signal is send to Experion [EN-54 part 2, 9.2.b] and the inhibit signal of the specific detector is sent to the Safety Manager logic. See for example FLD 101 (Figure 57 on page 138). For more details on M-out-of-N inhibit functionality, refer to the Fire and Gas Application manual.

Figure 57 FLD101 inhibit M-out-of-N function F&G detector devices

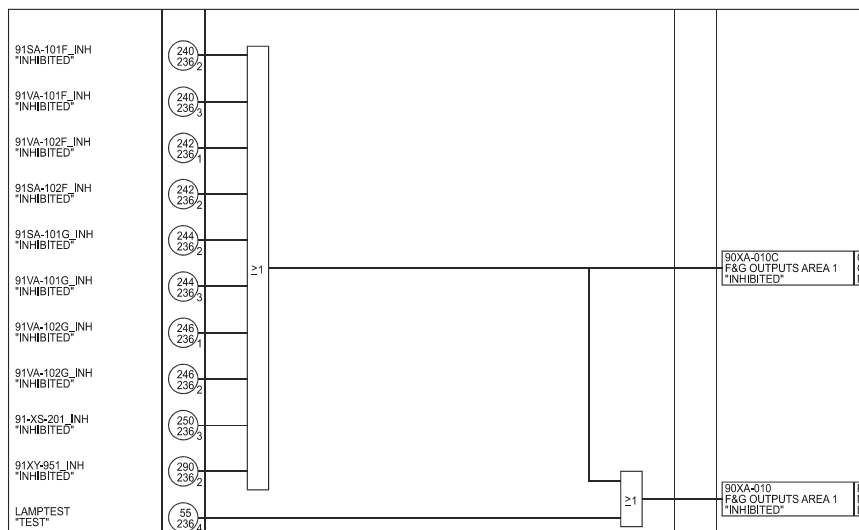


Inhibit signals are also grouped per area to generate a common inhibit indication per area on the F&G mimic panel and the overall display on the Experion console [EN-54 part 2, 9.2.a]. See FLD 234 (Figure 58 on page 139) for inhibited F&G detectors and FLD 236 (Figure 59 on page 139) for F&G inhibited outputs.

**Figure 58** FLD234 common F&G detector inhibited Area 1



**Figure 59** FLD236 common F&G outputs inhibited Area 1





# Special requirements for TUV-approved applications

# 10

Safety Manager can be used for processes which require, amongst others, TUV approval. The requirements for the safety applications are the following:

1. The maximum application cycle time is half the Process Safety Time. For example, the accepted Process Safety Time for a burner control system in accordance with TRD-411 for boilers > 30 kW (July 1985) Table 1, TRD-412 (July 1985) Table 1 and DIN 4788 (June 1977) Part 2 Chapter 3.2.3.2 1 is 1 second.

This implies that the application cycle time must be 0.5 second or less. The application cycle time is calculated by the SM Controller and can be seen on the **System Information** screen of Controller Management.

The application execution time is limited to 2 seconds by the hardware of the watchdog.

2. If Safety Manager detects a fault in its output hardware that is configured with Fault Reaction **Low**, it can de-energize parts of the process instead of de-energizing all outputs. The de-energization of process parts or all outputs is fully implemented in the software and cannot be influenced by the user (see also item 3). The de-energization depends on the output module type:

- SDO-0824      Safety Related digital output module  
(24 Vdc, 0.55 A, 8 channels)  
De-energization per group of output channels:  
Group 1: outputs 1, 2, 3, 4.  
Group 2: outputs 5, 6, 7, 8.
- SAO-0220m      Safety Related analog output module  
(0(4)-20 mA, 2 channels)  
De-energization per channel.
- SDO-04110      Safety Related digital output module  
(110 Vdc, 0.32 A, 4 channels)  
De-energization of group 1: outputs 1, 2, 3, 4.
- SDO-0448      Safety Related digital output module  
(48 Vdc, 0.75 A, 4 channels)  
De-energization of group 1: outputs 1, 2, 3, 4.
- SDO-0424      Safety Related digital output module  
(24 Vdc, 2 A, 4 channels)  
De-energization of group 1: outputs 1, 2  
De-energization of group 2: outputs 3, 4.
- SDOL-0424      Safety Related loop-monitored digital output module  
(24 Vdc, 1 A, 4 channels)  
De-energization of group 1: outputs 1 to 4.

If a complete output module (configured with Fault Reaction `Low`) is detected faulty, all outputs connected to the Control Processor that controls the output module are de-energized via the watchdog functionality of the Control Processor. If the output is located in a non-redundant IO section, all outputs of Safety Manager are de-energized. De-energization is only effected if safety-related outputs are allocated to the faulty module.

3. If Safety Manager detects a fault in its output hardware (configured with Fault Reaction `Low`, see item 2 above), a repair timer is started. When this timer expires, all outputs are de-energized via the watchdog functionality. This timer can be set to the following values:
  - Not used. The timer is not started so an output fault may be present in the system without further action.
  - 0 minutes. This results in immediate de-energization of all outputs in case of an output fault.
  - 0 hours to 2047 hours. This represents the interval time between the fault occurrence and automatic system shutdown.
4. If Safety Manager detects a fault in its input hardware (configured with Fault Reaction `Low`, `High`, `Bottom scale`, `Top scale`), the faulty input is set to its configured Fault Reaction state. This represents the safe status for digital and analog inputs.

5. The watchdog functionality of Safety Manager contains a shutdown (SD) input. For normal operation, the SD input must be 24 Vdc. If the input is forced to 0 V, a Safety Manager shutdown and de-energization of the outputs take place, independent of the QPP.
6. For more details on IO wiring details, termination of IO signals and power supply distribution see *Hardware Reference*.
7. The Diagnostic Test Interval (DTI, the time in which all IO tests are executed) can be set for each SM Controller in the Controller Properties in the Network Configurator.
8. The repair timer can be set for each SM Controller in the Controller Properties in the Hardware Configurator.
9. The values of the voltage monitor analog input channels of the SAI-1620m modules must be checked in the application to ensure that they are within the transmitter power supply range of the transmitters connected to that analog input module.
10. To reduce the influence of disturbances on the power supply lines, all major metal parts (cabinet sidewalls, doors, 19-inch chassis, horizontal bus chassis and flaps, swing frames, etc.) must be properly grounded.
11. All power supply inputs (except 110/230 Vac) require a power supply filter directly fitted after the power supply input terminals.
12. Grounding of the power supplies of Safety Manager is only permitted for the 0 Vdc. Grounding of the +24 Vdc / +48 Vdc / +60 Vdc / +110 Vdc is not allowed because an earth fault results in an unsafe situation.
13. The wiring of the external power supply (24 Vdc) and the internal power supply (5 Vdc) must be physically separated. This can be realized by using separate ducts and a separate power supply distribution.
14. Do not use radio frequency transmitting equipment within a radius of 1 m (3 ft) of the system cabinet when the doors are opened.
15. Safety-related inputs require the use of tested input modules (SDI-1624, SDI-1648, SAI-1620mm, SAI-0410, or SDIL-1608) and safety-related input sensors (transmitters). If the input sensors (transmitters) are not safety related, redundant sensors (transmitters) must be used.
16. If Safety Manager operates without operator surveillance, some measures have to be taken. During the design and implementation stages of the safety system a reliability calculation analysis (the maximum time period in which inspection has to take place) has to be performed. Without operator

surveillance the following measures have to be taken to comply with the safety integrity requirements:

- Inspection of Safety Manager status if the Safety Manager application is fault free, at least once per determined time period.
- Alarm indication of Safety Manager if a fault is detected and subsequent inspection of the Safety Manager status within the safety determined time period.

17. The operating conditions of Safety Manager shall not exceed the following ranges:

- Operating temperature: -5 to 70°C
- Relative humidity: 5% to 95%, non-condensing
- Vibration: 1G (10-55-10 Hz)
- Shock: 15 G (11 ms, 3 axes, both directions of the axe)
- Supply voltage: 110 Vdc (+25% / -15%), 48 Vdc (+15% / - 15%), 24 Vdc (+30% / -15%)

For details refer to *Hardware Reference*.

The operating temperature is measured in Safety Manager. This temperature is higher than the temperature outside the cabinet, which results in a lower ambient temperature for the cabinet. Depending on the internal dissipation in the cabinet and the ventilation, a temperature difference of 25°C (77°F) is allowed, which results in a maximum ambient temperature of 45°C (113°F). To minimize the temperature difference, forced ventilation with one or more fans may be required. By using the temperature pre-alarm setpoints, an alarm can be given if the internal temperature is too high.

18. The storage conditions of the Safety Manager hardware modules shall not exceed the following ranges:

Storage temperature: -25 to +80°C (-13 to 176°F).

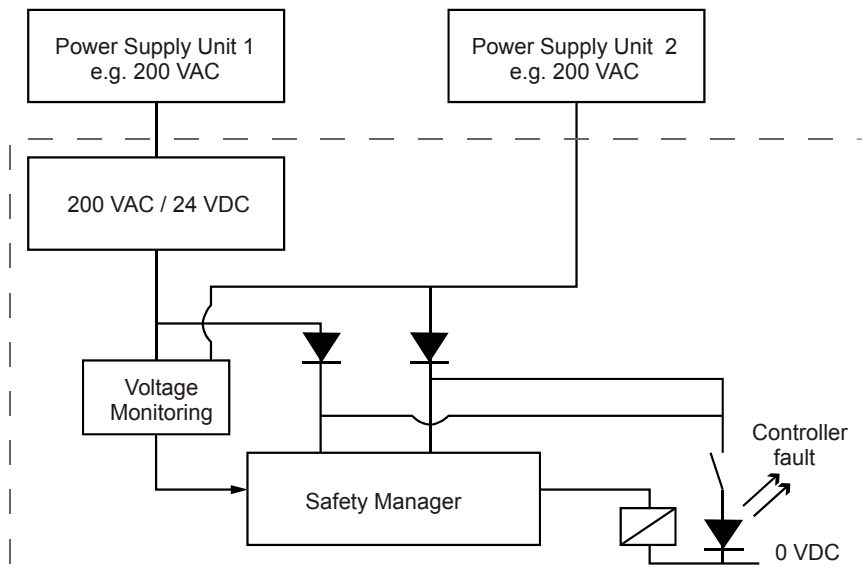
## F&G applications

Fire and Gas (F&G) applications have the following additional requirements:

1. Each visual indication (alarm, override or test, failure) shall have its own dedicated digital output. This digital output may be a hardware output or a communication output, e.g. to a DCS system. Override and test status may be combined in one visual indication. Alphanumeric displays are not supported.
2. Redundant power supplies must be connected to Safety Manager in such a way that the redundant power supplies do not fail at the same time, e.g. by using different primary power sources (e.g. 220 Vac mains and a 24 Vdc from a battery backup). Detection of power supply failure (e.g. via a voltage-monitoring module) shall be part of the system design.



**Figure 60** Power supply



3. Faults in the Fire & Gas detection system are indicated visually. This indication must also be active if the Fire & Gas detection system has been switched off. This can be set up as shown in Figure 60 on page 145, using a normally de-energized relay, or via a visual indication in a DCS display which is activated if the communication to the Fire & Gas detection system fails. The protected side of the fuses is connected to a voltage-monitoring device to detect blown fuses.
4. The field instruments, including panel instruments such as (key) switches, which are used in conjunction with Safety Manager, must meet the requirements of the applicable parts of the EN-54 standard. Visual and audible indications shall be as defined in paragraph 3.2 of EN-54 part 2.
5. Field inputs must have loop-monitoring to detect short-circuits and open loops. Input module types that can be used are: SAI-0410, SAI-1620m and SDIL-1608.  
Field outputs must also have loop-monitoring. Output module type that can be used: SDOL-0424.
6. The Fire & Gas detection system shall have earth leakage monitoring/detection facilities.
7. Remote display of alarms, failures etc. may only be given via interconnection of Safety Manager systems using the communication option between Safety Manager systems or via hard wired outputs with loop-monitoring via the

SDOL-0424 digital output modules. Communication and loop monitoring failures must be alarmed.

8. Safety Manager is only the basis for an EN-54 compliant application. The responsibility for a full EN-54 compliant application lies with the person(s) responsible for configuring and application programming of Safety Manager. The requirements of EN-54 which must be met by the application can be found in section 9, which references the requirements that must be fulfilled in the application.
9. For details on the requirements of the mechanical construction (cabinet, indications, horns) refer to “EN-54 part 2 paragraph 3.2.”

# List of abbreviations

<b>AI</b>	Analog Input
<b>AO</b>	Analog Output
<b>ASM</b>	Abnormal Situation Management
<b>BKM</b>	Battery and Key switch Module
<b>BMS</b>	Burner Management System
<b>CP</b>	Control Processor
<b>DCS</b>	Distributed Control System
<b>DI</b>	Digital Input
<b>DO</b>	Digital Output
<b>DTI</b>	Diagnostic Test Interval
<b>E/E/PES</b>	Electrical/Electronic/Programmable Electronic System
<b>EMC</b>	Electromagnetic Compatibility
<b>ESD</b>	<ul style="list-style-type: none"> <li>• Electrostatic Discharge</li> <li>• Emergency ShutDown system</li> </ul>
<b>EUC</b>	Equipment Under Control
<b>EUT</b>	Equipment Under Test
<b>F&amp;G</b>	Fire and Gas
<b>FB</b>	Function Block
<b>FGS</b>	Fire and Gas System
<b>FLD</b>	Functional Logic Diagram
<b>FTA</b>	Field Termination Assembly
<b>FTE</b>	Fault Tolerant Ethernet
<b>HIPS</b>	High-Integrity Protection Systems
<b>HMI</b>	Human Machine Interface
<b>HSE</b>	High Speed Ethernet
<b>IO</b>	Input/Output
<b>IP</b>	<ul style="list-style-type: none"> <li>• Internet Protocol</li> <li>• Ingress Protection</li> </ul>
<b>IS</b>	Intrinsically Safe
<b>LAN</b>	Local Area Network
<b>LED</b>	Light-Emitting Diode
<b>MAC</b>	Media Access Control
<b>MAP</b>	Manufacturing Automation Protocol

*List of abbreviations*

<b>MOS</b>	Maintenance Override Switch
<b>MTBF</b>	Mean Time Between Failure
<b>MTTF</b>	Mean Time To Failure
<b>MTTR</b>	Mean Time To Repair
<b>OLE</b>	Object Linking and Embedding
<b>OPC</b>	Object linking and embedding for Process Control
<b>OS</b>	Operating System
<b>P&amp;ID</b>	Piping and Instrumentation Diagram
<b>PE</b>	Protective Earth
<b>PES</b>	Programmable Electronic System
<b>PFD</b>	Probability of Failure on Demand
<b>PKS</b>	Process Knowledge System
<b>PLC</b>	Programmable Logic Controller
<b>PST</b>	Process Safety Time
<b>PSU</b>	Power Supply Unit
<b>PUC</b>	Process Under Control
<b>PV</b>	Process Value
<b>QMR</b>	Quadruple Modular Redundant
<b>QPP</b>	Quad Processor Pack
<b>RFI</b>	Radio Frequency Interference
<b>SCADA</b>	Supervisory Control And Data Acquisition
<b>SIC</b>	System Interconnection Cable
<b>SIL</b>	Safety Integrity Level
<b>SIS</b>	Safety Instrumented System
<b>SMOD</b>	Secondary Means Of De-energization
<b>SRS</b>	Safety-Related System
<b>USI</b>	Universal Safety Interface
<b>UTP</b>	Unshielded Twisted Pair
<b>WAN</b>	Wide Area Network

# Safety Manager Glossary

## A

### **Alarm**

An automatic signal that serves as a warning of an event or danger.

### **Application**

The definition of the EUC-dependent function for Safety Manager.

### **Application Compiler**

A tool of the Safety Builder used to create a controller file.

### **Application Editor**

A tool of the Safety Builder used to create or edit functional logic diagrams.

### **Application value**

The value of a process Point as provided to, or calculated by, the application software.

### **Application Viewer**

A tool of the Safety Builder used to view functional logic diagrams on-line.

### **Availability**

- The ratio of system up time to total operating time.
- The ability of an item to perform its designated function when required for use.

## B

### **Battery and Key switch Module (BKM)**

A module in the SM Controller used to:

- Supply battery power to the system memory (RAM) and the real time clock of the Control Processor modules, in case of power outage.
- Enable or disable forces, by turning the Force key switch. When enabled, forcing of certain input and output signals is allowed. When disabled, all forces are removed.
- Provide a fault reset, by turning the Reset key switch. See Fault reset.



#### **Warning**

Turning the Reset key switch during an On-Line Modification procedure may cause the Control Processors to swap status.

---

## C

### **Communication module**

See: Universal Safety Interface (USI)

### **Communication time-out**

An error caused by an unacceptable large time interval during which there was no communication.

### **Control Processor (CP)**

Core component of the SM Controller consisting of: Power Supply Unit (PSU), Quadruple Processor Pack (QPP) and 1 or 2 communication modules (USI).

### **Controller chassis**

19" chassis to slot the BKM and Control Processor modules.

### **Controller Management**

A tool of the Safety Builder used to perform the following functions:

- Load controller.
- View system status.
- Retrieve controller and application files.

### **Cycle time**

The time period needed to execute the application software once.

## D

**Database Rebuilder**

Repair function for the information storage for Safety Builder created databases.

**Deutsches Institut für Normung (DIN)**

German Institute for Standards, which determines the standards for electrical and other equipment in Germany.

**Diagnostic Test Interval (DTI)**

The time period used by Safety Manager to cyclically locate and isolate safety related faults within on-line system components that could otherwise cause a hazardous situation. See also “Process Safety Time (PST)” on page 160.

Within Safety Manager, the default DTI is set at three seconds.

**Distributed Control System (DCS)**

System designed to control industrial processes. A DCS receives the measured values of the process instrumentation, e.g. flow, pressure, temperature. It controls the process via analog control equipment such as control valves. In addition, a DCS may receive many digital signals for alarm and management purposes.

**Dual Modular Redundant (DMR)**

Safety configuration providing 1oo2 configuration. The DMR technology is used in the architecture of a non redundant QPP where on-board 1oo2D voting is based on dual-processor technology.

DMR is characterized by a high level of diagnostics and fault coverage.

## E

**Electrical/Electronic/Programmable Electronic (E/E/PE) device**

A device based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology.

**Note**

This term is intended to cover any and all devices operating on electrical principles and would include:

- electro-mechanical devices (“electrical”);
  - solid state non-programmable electronic devices (“electronic”);
  - electronic devices based on computer technology (“programmable electronic”).
-

### **Electrical/Electronic/Programmable Electronic system (E/E/PES)**

A system based on one or more E/E/PE devices, connected to (and including) input devices (e.g. sensors) and/or output devices/final elements (e.g. actuators), for the purpose of control, protection or monitoring.

See also: “Programmable Electronic System (PES)” on page 160.

### **Electromagnetic Compatibility (EMC)**

The ability of a device, equipment or system to function satisfactory in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.

### **Electrostatic discharge (ESD)**

The transfer of electrostatic charge between bodies of different electrostatic potential, which may cause damage to system components.

### **Emergency Shutdown (ESD)**

Manual or automatic turning off or closing down of process equipment in case of anomalous conditions in order to prevent damage to the system or process.

### **Equipment Under Control (EUC)**

Equipment/machinery/apparatus/Plant used for manufacturing, process, transportation, medical or other activities for which designated safety-related systems could be used to:

- prevent hazardous events associated with the EUC from taking place; or,
- mitigate the effects of the hazardous events.

### **Error**

See the *Safety Manual*.

### **Ethernet**

A local area network specification developed by Xerox in 1976. The specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers of the network. It uses CSMA/CD to handle simultaneous transmissions and is the most popular LAN Technology in use today. More commonly used to reference an Ethernet Network running at 10 Mb/s.

See also: Local Area Network (LAN).

### **Event**

- Occurrence of some programmed action within a process which can affect another process.
- Asynchronous occurrence that is detected by the control system, time and other information is recorded, e.g. process alarm.



### **Experion PKS**

Honeywell Process Knowledge System™ for process, business and asset management.

### **Experion PKS Station**

Windows 2000/XP based station for viewing process schematics and interactions with the system. This station provides comprehensive alarm and event detection, management, reporting facilities, and history collection along with the capability of custom process graphics.

### **External risk reduction measures**

Physical measures taken externally to safety-related systems to reduce or mitigate the risks. Examples would include a drain system, fire wall, etc.

## **F**

### **Failure**

See the *Safety Manual*.

### **Fault**

See the *Safety Manual*.

### **Fault reset**

An action that clears the fault database and attempts a restart of tripped or halted components of the system.

### **Fault Tolerant Ethernet (FTE)**

Experion PKS patented advanced networking solution that delivers greater system availability.

### **FC**

Prefix used to identify conformal-coated module from non conformal coated modules. See also: FS.

- FC-SDI-1624 is a safe digital input module with conformal coating
- FS-SDI-1624 is a safe digital input module without conformal coating

### **Field Termination Assembly (FTA)**

Assembly to connect field wiring to the SM IO modules.

### **Field value**

The value of a process Point as present at the interface of the system with the EUC.

### **Fieldbus**

Wiring solution and communication protocol in which multiple sensors and actuators are connected to a DCS or SIS, using a single cable.

### **Fire and Gas system**

Independent protective system which continuously monitors certain process Points (e.g. combustible gas levels) and environmental Points (e.g. heat, smoke, temperature and toxic gas levels). If any of these Points exceed a predetermined level, the system will raise an alarm and take automatic action to close operating valves and damper doors, activate extinguishers, cut off electrical power and vent dangerous gases.

### **Force**

A signal override of some sort that is applied on a system level.

A force applied to an input affects the input application state as it overrides the actual field value and diagnostic state of the forced input.

A force applied to an output affects the output field state as it overrides the application value or diagnostic value with the forced value.



### **Caution**

Forcing introduces a potentially dangerous situation as the corresponding Point could go unnoticed to the unsafe state while the force is active.

---

### **FS**

Prefix used to identify non conformal-coated module from conformal coated modules. See also: FC.

- FS-SDI-1624 is a safe digital input module without conformal coating
- FC-SDI-1624 is a safe digital input module with conformal coating

### **Function block**

Element in a functional logic diagram (FLD) which performs a user defined logic function. Function blocks are designed to implement & re-use complex functions via a single (user defined) element.

### **Functional Logic Diagram (FLD)**

Diagrammatic representation of the application (conform the IEC 61131-3 standard) which is used to program Safety Manager. FLDs are directly translated into code that can be executed by Safety Manager, thus eliminating the need for manual programming. See also: Application Editor.

### **Functional safety**

See the *Safety Manual*.

### **Functional safety assessment**

See the *Safety Manual*.

## **H**

### **Hardware Configurator**

A tool of the Safety Builder used to configure the hardware of Safety Manager.

### **Hardware safety integrity**

See the *Safety Manual*.

### **Hazard**

A physical situation with a potential for human injury.



#### **Note**

The term includes danger to persons arising within a short time scale (e.g. fire and explosion) and also those that have a long-term effect on a persons health (e.g. release of a toxic substance).

---

### **High voltage**

A voltage of 30VAC, 40VDC or above.

## **I**

### **IEC 61131-3**

Part of the international standard IEC 61131, which provides a complete collection of standards on programmable controllers and their associated peripherals.

The IEC 61131-3 specifies the syntax and semantics of programming languages for programmable controllers as defined in part 1 of IEC 61131 (FLD symbols).

### **IEC 61508**

International IEC standard on functional safety entitled “Functional safety: safety-related systems”, which sets out a generic approach for all electrically based systems that are used to perform safety functions. A major objective of this international standard is to facilitate the development of application sector standards.

**Institute of Electrical and Electronic Engineers (IEEE)**

An American professional organization of scientists and engineers whose purpose is the advancement of electrical engineering, electronics and allied branches of engineering and science. It also acts as a standardization body.

**International Electrotechnical Commission (IEC)**

An international standards development and certification group in the area of electronics and electrical engineering, including industrial process measurement, control and safety.

**Interval time between faults**

See: Repair time.

**IO bus**

A bus-structure within Safety Manager that interconnects the Control Processor with the IO.

**IO bus driver**

Part of the Quad Processor Pack that controls the IO bus.

**IO chassis**

19" chassis to slot the (redundant) IO extender(s) and SM IO modules.

**IO database**

Database in which input, output and configuration data is stored.

**IO extender**

Module which controls the IO bus of the IO chassis. A maximum of ten IO extender modules can be connected to one IO bus.

**IO module**

Module which handles input or output functions of Safety Manager. IO modules can be digital or analog.

**L**

**Local Area Network (LAN)**

A general term to refer to the network and its components that are local to a particular set of devices.

See also: Wide area network (WAN).

## M

**Maintenance override**

A function, which allows the user to apply an application value to an input independent of the input channel scan value.

**Maintenance Override Switch (MOS)**

Switch used to file a request for a maintenance override. Acknowledgement is decided by the application program. An acknowledged maintenance override allows maintenance to be performed on field sensors or field inputs without causing the safety system to trip the process.

**Master-clock source**

The source that is responsible for the time synchronization between a group of systems or within a network.

**Mean Time Between Failure (MTBF)**

- For a stated period in the life of a functional unit, the mean value of the length of time between consecutive failures under stated conditions.
- The expected or observed time between consecutive failures in a system or component.

MTBF is used for items which involve repair.

See also: Mean Time To Repair (MTTR), Mean Time To Failure (MTTF).

**Mean Time To Failure (MTTF)**

The average time the system or component of the system works without failing.

MTTF is used for items with no repair.

See also: Mean Time To Repair (MTTR), Mean Time Between Failure (MTBF).

**Mean Time To Repair (MTTR)**

The mean time to repair a safety-related system, or part thereof. This time is measured from the time the failure occurs to the time the repair is completed.

**Media Access Control (MAC)**

The lower sublayer of the data link layer (Layer 2) unique to each IEEE 802 local area network. MAC provides a mechanism by which users access (share) the network.

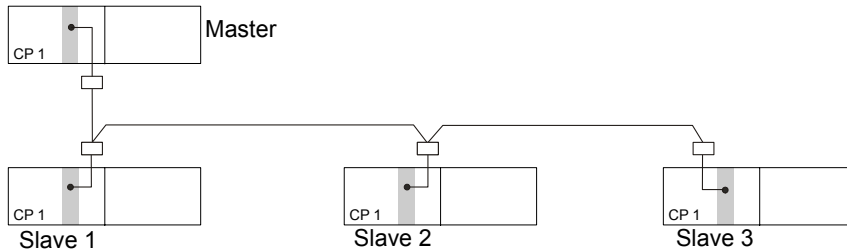
**Mode of operation**

See the *Safety Manual*.

## Multidrop link

A multidrop link is a physical link that interconnects multiple systems (see Figure Figure 61 on page 158).

**Figure 61** Multidrop link



## N

### Namur

A 2-wire proximity switch operating at a working voltage of 8.2 V and an operating current of 8mA max (CENELEC Standard). Because of the small amount of energy needed to operate NAMUR sensors, they can be used in intrinsically safe applications.



#### Note

Special switching amplifiers or dedicated input modules, like the SDIL-1624, are required to read the status of NAMUR proximity switches.

### Network Configurator

A tool of the Safety Builder used to configure the communication architecture.

### Node

Hardware entity connected to a network.

## O

### Object linking and embedding for Process Control (OPC)

Technology developed originally by Microsoft, now being standardized. Microsoft technology for application interoperability. Object Linking and Embedding (OLE) is a set of services that provides a powerful means to create documents consisting of multiple sources of information from different applications. Objects can be almost any type of information, including text, bitmap images, vector graphics, voice, or video clips.

**Off-line**

A system is said to be “off-line” when it is not in active control of equipment or a process.

A process or equipment is said to be “off-line” when it is in shut-down.

**On-line**

A system is said to be “on-line” when it is in active control of equipment or a process.

A process or equipment is said to be “on-line” when it is operating.

**Operational state**

The values of an application Point during normal process operation.

**P****Peer-to-peer**

A logical connection between two points.

**Plant**

A component of Safety Builder which represents a collection of devices, controllers and communication networks interconnecting the devices and controllers.

**Point**

A data structure in the IO database, usually containing information about a field entity. A point can contain one or more parameters. Safety Manager uses different point types to represent a range of different field values.

**Point Configurator**

A tool of the Safety Builder used to create and modify Points of a SM Controller.

**Point Viewer**

A tool of the Safety Builder used to view Points with dynamic update of states and values.

**Power Supply Unit (PSU)**

Separate module which supplies electrical power to the SM Controller.

**Probability of Failure on Demand (PFD)**

A value that indicates the probability of a system failing to respond to a demand. PFD equals 1 minus Safety Availability. (ISA, S84.01, 1996)

**Process Safety Time (PST)**

The time that a process can tolerate a faulty situation without causing a hazardous situation. See also “Diagnostic Test Interval (DTI)” on page 151.

**Process value**

An amount, expressed in engineering units, that represents the value of a process variable, e.g. a temperature, a pressure or a flow.

**Programmable Electronic System (PES)**

See the *Safety Manual*.

**Programmable Electronics (PE)**

See the *Safety Manual*.

**Q****Quad Processor Pack (QPP)**

The main processing module of the SM Controller.

**Quadruple Modular Redundant (QMR)**

Safety configuration providing a 2oo4D configuration. The QMR technology is used in the architecture of a redundant QPP where on-board 1oo2D voting (see Dual Modular Redundant (DMR)) is combined with 1oo2D voting between the two QPPs.

Voting takes place on two levels: First on a module level and secondly between the Control Processors.

QMR is characterized by a high level of diagnostics, fault coverage and fault tolerance.

**R****Redundancy**

- In an item, the existence of more than one means of performing a required function.
- Use of duplicate (or triple or quadruple) modules or devices to minimize the chance that a failure might disable an entire system.

**Repair time**

- The time required to identify the location of a fault and repair the fault.
- A time window allowed by the system to identify the location of a fault and repair the fault. If the repair is not successfully completed within the given time window a trip is to be expected.



**Repair timer**

A count-down timer that starts if a fault has been detected which degrades the existing safety level of Safety Manager.

A repair timer keeps track of the remaining repair time (see Repair time) and can only be reset by repairing the fault that initiated the timer.

If a repair timer runs out, the corresponding Control Processor halts.

**Reset**

See: Fault reset.

**Risk**

See the *Safety Manual*.

**Router**

A network device which forwards packets (messages or fragments of messages) between networks.

The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.

**S****Safety**

See the *Safety Manual*.

**Safety Availability**

The fraction of time (%) that a safety system is able to perform its designated safety service when the process is operating. See also “Probability of Failure on Demand (PFD)” on page 159.

**Safety Builder**

Station software used to configure, design, validate, log and monitor a Safety Manager project.

**Safety integrity**

See the *Safety Manual*.

**Safety Integrity Level (SIL)**

See the *Safety Manual*.

**Safety life cycle**

See the *Safety Manual*.

### **Safety Manager**

A safety solution to protect the integrity of the process. Safety Manager includes the following components:

- Safety Manager
- Safety Station

For details see the *Overview Guide*.

### **Safety-related system (SRS)**

See the *Safety Manual*.

### **Safety Station**

Station running Safety Builder and Safety Historian.

### **Second fault timer**

See: Repair timer.

### **Secondary Means Of De-energization (SMOD)**

Auxiliary transistor on the output module, which is de-energized in case a “stuck at” failure occurs at one of the output transistors (due to random hardware failures). This results in a safe state for the output.

### **Shutdown**

A process by which an operating Plant or system is brought to a non-operational state.

### **SICC**

IO signal wiring using system interconnection cables that hook up the FTA board to the IO.

### **SICP**

IO signal wiring using system interconnection cables that hook up the screw terminals to the IO.

### **SM Controller**

Assembly of Control Processor, Controller chassis and BKM. A Controller can be redundant or non redundant. A redundant Controller contains two Control Processors. A non redundant Controller contains one Control Processor. Note that IO is not included.

### **SM IO**

A set of IO chassis linked to a Safety Manager Controller.

### **Safety Manager**

An Safety Manager comprises the following subsystems:

- SM Controller
- SM IO
- FTA

For details see the *Overview Guide*.

### **Switch**

A network device which forwards packets (messages or fragments of messages) by means of packet switching.

The forwarding decision is based on the most expedient route (as determined by some routing algorithm). Not all packets travelling between the same two hosts, even those from a single message, will necessarily follow the same route.

### **System Interconnection Cable (SIC)**

Cables to connect IO modules with FTAs or terminals.

## **T**

### **Timestamp**

As a verb, the act of putting the current time together with an event. As a noun, the time value held with an event.

### **Trend**

A display defined primarily for presentation of and navigation through historical information.

### **Trip**

An action by which part of an operating Plant or system is brought to a non-operational state.

See also: Shutdown.

### **Triple Modular Redundant (TMR)**

Safety technology which is based on comparison principles and which requires triplicated system components.

## **U**

### **Universal Safety Interface (USI)**

Communication module of the SM Controller.

## V

### Validation

See the *Safety Manual*.

### Verification

Confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled.



#### Note

In the context of IEC 61508, verification means the process of demonstrating for each phase of the relevant safety lifecycle (overall, E/E/PES, software), by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

Examples of verification activities would include:

1. Reviews on deliverables (documents from all phases of the safety lifecycle) to ensure compliance with the objectives and requirements of the phase taking into account the specific inputs to that phase.
  2. Design reviews.
  3. Tests performed on the designed products to ensure that they perform according to their specifications.
  4. Integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.
- 

### Voting configuration

To prevent that a safety-related system remains passive or false signals occur in this system it is possible to use voting. With voting the safety-related system makes a decision based on signals. The usage of more than one signal enhances the safety and reliability of the system.

## W

### Watchdog

A combination of diagnostics and an output device (typically a switch) the aim of which is to monitor the correct operation of the programmable electronic (PE) devices and takes action upon detection of an incorrect operation.



#### Note

The watchdog is used to de-energize a group of safety outputs when dangerous failures are detected in order to put the EUC into a safe state. The watchdog is used to increase the on-line diagnostic coverage of the logic system

---

**Wide area network (WAN)**

A general term to refer to a piece of a network and its components that are used to inter-connect multiple LANs over a wide area.



# Index

## A

- alarm markers 114
  - behavior 82
  - FaultReset 114
  - normal state 82
- alarms 133
- allocation IO signals 59
- analog input faults 87
- Analog inputs (AI)
  - Synchronization 93
- analog output faults 89
- application 55, 60, 118, 141
  - database 55, 60
  - program cycle time 141
  - software implementation 60
- application design 6
- architectures Safety Manager 30
- availability 30

## B

- basic skills and knowledge 3
- BKM faults 99

## C

- calculation errors 102
  - calculated value outside specified range 102
  - counter outside specified range 102
  - divide by zero 102
  - function blocks 104
  - overflow 102
  - prevention 102
  - square root negative number 102
- Canadian Standards Association (CSA) 12
- CE compliance 11
- CE marking 16
- channel status 83
- clearing all forces 66

- communication 49
  - ~ link 49
- communication faults 100
- compare error 92
- compatibility check 68
  - on-line modification 68
- compliance standards 11, 13, 16
- configurations Safety Manager 30, 31, 32, 33, 35, 37
  - availability requirements 30
  - basic architectures 30
  - Dual Modular Redundant (DMR)
    - architecture 30
  - non-redundant Controller, non-redundant IO 32
  - Quadruple Modular Redundant (QMR)
    - architecture 31
  - redundant Controller, non-redundant IO 33
  - redundant Controller, redundant IO 35
  - redundant Controller, redundant IO, non-redundant IO 37
- connections safety system 47
- continuous mode of operation 23, 25
- Controller properties 57, 58
  - diagnostic test interval 58
  - maximum repair time 58
  - safety integrity level 57
- cycle time 141

## D

- dangerous failure 20
- databases 55, 60
  - IO database 55
- de-energization 141, 142
- deluge valve 126
- design phases 42
  - ESD system 42
  - safety system 42
- detector 122
- detectors 119

- diagnostic inputs 80, 83, 113
  - LoopI 84
  - LoopO 84
  - SensAI 84
- diagnostic message 74
- diagnostic test interval 58, 141
  - Controller properties 58
- diagnostics
  - calculation errors 103
- digital input faults 86
- Digital inputs (I)
  - Synchronization 93
- digital output faults 87
- directives 16, 17, 18
  - EMC directive (89/336/EEC) 17
  - low voltage directive (73/23/EEC) 18
- DTI 58, 141
  - Controller properties 58
- Dual Modular Redundant (DMR) 30

## E

- earth leakage monitoring/detection 145
- Electromagnetic Compatibility (EMC) 17
- electromagnetic disturbance 17
- EMC directive (89/336/EEC) 17
- emergency shutdown (ESD) 110, 143
  - input 143
- emergency shutdown systems 4
- Equipment Under Control (EUC) 4
- error 20, 22
  - human ~ 22
- ESD system 42
  - design phases 42
- EU directives 16, 17, 18
- EUC risk 20
- European Committee for Standardization 11
- European Economic Area (EEA) 17, 18
- European Union 16, 17, 18

## F

- F&G
  - alarms 133
  - deluge valve 126
  - firewater pumps 128
  - HVAC system 130
  - PA/GA system 130

- F&G detectors 119
- Factory Mutual (FM) 12
- failure 20, 24, 58
  - dangerous ~ 20
  - isolation 58
  - safe ~ 24
- fault 21, 69, 136, 142
  - database 74
  - detection 70, 73
  - reaction 70
  - reaction state 75
  - repair 79
  - response 70
  - timer 142
- fault detection
  - cycle 74
- fault detection and response
  - behavior alarm markers 82
- faults
  - analog input 87
  - analog output 89
  - BKM 99
  - calculation errors 102
  - communication 100
  - digital input 86
  - digital output 87
  - IO compare 92
  - PSU 100
  - QPP 97
  - USI 99
- field instruments 145
- filters 143
- Fire & Gas 118
- fire and gas detection systems 4
- Fire&Gas (F&G) applications 144, 145
  - earth leakage monitoring/detection 145
  - field instruments 145
  - loop-monitoring 145
  - redundant power supplies 144
  - remote display 145
  - requirements 144
- firewater pumps 128
- force
  - clear all 66
  - key switch 66
- forcing inputs/outputs 66
  - clearing all forces 66
- function blocks
  - calculation errors 104



Functional Block Diagram 6  
 functional logic diagrams (FLDs) 49, 56  
 functional safety 21  
 functional safety assessment 22  
 functional safety standards 11

## G

grounding 143

## H

hardware safety integrity 22  
 hazard analysis 7  
 high demand mode of operation 23, 25  
 human error 22  
 humidity 144  
   relative ~ 144  
 HVAC system 130

## I

IEC 61131-3 11  
 IEC 61508 4, 7  
 IEC 61511 4, 7, 8  
 implementation 60  
   application software 60  
 inhibit 138  
 input filters 143  
 input signals 59  
   physical allocation 59  
 Input synchronization  
   Analog inputs 93  
   Digital inputs 93  
 inputs 66  
   clearing all forces 66  
 Instrument Society of America (ISA) 11  
 instrumentation 47  
   ~ index 47  
   safety system 47  
 International Electrotechnical Commission (IEC) 11  
 interval time between faults 58  
 IO compare faults 92  
 IO database 55, 60  
 IO signals 59  
   physical allocation 59  
 isolate 70

## L

ladder diagram 6  
 line-monitored 125  
 Lloyds Register of Shipping 12  
 logical functions (in FLDs) 49  
 loop status 84  
 LoopI diagnostic input 84  
 loop-monitoring 145  
 LoopO diagnostic input 84  
 low demand mode of operation 23, 25  
 low voltage directive (73/23/EEC) 18

## M

marker  
   diagnostic 74  
   diagnostic message 74  
 markers  
   alarm 74, 80, 81  
   state 82  
   system 80  
 mode of operation 23, 25  
   continuous ~ 23, 25  
   high demand ~ 23, 25  
   low demand ~ 23, 25

## N

non-redundant Controller, non-redundant IO 32

## O

on-line modification (OLM) 68  
   compatibility check 68  
 operating conditions 144  
   operating temperature 144  
   relative humidity 144  
   shock 144  
   vibration 144  
 operator surveillance 143, 144  
 output signals 59  
   physical allocation 59  
 outputs 66  
   clearing all forces 66

## P

- PA/GA system 130
- phases 42
  - ESD system 42
  - safety system 42
- physical allocation 59
  - Safety Manager 59
- points 66
  - clearing all forces 66
- power supply 143, 144
  - ~ failure 144
  - ~ filters 143
  - redundant unit (PSU) 144
- power supply unit (PSU) 144
  - redundant 144
- prerequisite skills 3
- process 48, 111, 112
  - ~ interface 48
  - ~ outputs (in unit shutdown) 112
  - ~ units 111
- Process safety time 70
- Process Under Control (PUC) 4, 5
- Programmable Electronic System (PES) 23
- PSU faults 100

## Q

- QPP faults 97
- Quad Processor Pack (QPP) 32
  - watchdog 32
- Quadruple Modular Redundant (QMR) 31

## R

- radio interference 143
- redundant 144
  - power supplies 144
- redundant Controller, non-redundant IO 33
- redundant Controller, redundant IO 35
- redundant Controller, redundant IO,
  - non-redundant IO 37
- registers
  - alarm 82
  - system 81
- relative humidity 144
- remote display 145
- Repair time 71

- repair timer 71, 77, 142
- risk 24
- risk assessment 7
- risk reduction measures 40

## S

- Safe 71
- safe failure 24
- safety 21, 24
  - functional ~ 21
- Safety Builder 54, 56
  - functions 56
- safety integrity 22, 28
  - hardware ~ 22
  - systematic ~ 28
- Safety Integrity Level 69
- Safety Integrity Level (SIL) 4
- safety integrity level (SIL) 57
- safety life cycle 26, 39, 40, 42, 44
  - E/E/PES 40
  - objectives 42
  - phases 42
  - sequence of phases 44
  - software 40
- Safety Manager 11, 59
  - physical allocation 59
  - standards compliance 11
- Safety Manager
  - configurations 30, 31, 32, 33, 35, 37
  - availability requirements 30
  - basic architectures 30
  - Dual Modular Redundant (DMR)
    - architecture 30
  - non-redundant Controller, non-redundant IO 32
  - Quadruple Modular Redundant (QMR)
    - architecture 31
  - redundant Controller, non-redundant IO 33
  - redundant Controller, redundant IO 35
  - redundant Controller, redundant IO,
    - non-redundant IO 37
- Safety related 71
- safety relation 113
- safety standards 11, 13, 16
- safety system 42, 47, 48, 49
  - connections 47
  - design phases 42

- function 49
- instrumentation 47
- process interface 48
- safety system specification 47, 48, 49, 51
  - approval 51
  - connections 47
  - functional logic diagrams (FLDs) 49
  - functionality 49
  - IO signals 48
- safety time 143
- safety-related inputs 143
- safety-related system 26
- Secondary Means 71
- Secondary Means of De-energization (SMOD) 32
- self-tests 58
- SensAI diagnostic input 84
- shock 144
- shutdown 110, 111, 112, 113
  - emergency ~ (ESD) 110
  - unit ~ 111, 112, 113
- Single fault tolerant 72
- SIS 69
- SMOD 71
- smoke detectors 119
- sounders and beacons 125
- standards compliance 11, 13, 16
- states
  - Control Processor 72
  - IO 73
  - process 73
- status
  - channel 83
  - loop 84
- storage conditions 144
- structured text 6
- Synchronization
  - Analog inputs 93
  - Digital inputs 93
- synchronize 91, 92, 93
- system configuration parameters 57
- systematic safety integrity 28
- systems 30, 31, 32, 33, 35, 37
  - basic architectures 30
  - Dual Modular Redundant (DMR) architecture 30
  - non-redundant Controller, non-redundant IO 32

- Quadruple Modular Redundant (QMR) architecture 31
- redundant Controller, non-redundant IO 33
- redundant Controller, redundant IO 35
- redundant Controller, redundant IO, non-redundant IO 37

## T

- tag numbers 47
  - description 47
  - status 47
- temperature 144
  - operating ~ 144
- textual languages 6
- time functions (in FLDs) 49
- time-out 101
- timer 142
  - fault 142
- TUV 12

## U

- UL 1998 11
- Underwriters Laboratories (UL) 12
- unit relays 112
- unit shutdown 111, 112, 113
  - ~ outputs 112
  - application programming 113
  - configuration 111
  - diagnostic inputs 113
  - process outputs (safety-related) 112
  - safety relation of outputs 113
- unit shutdown outputs 112
- USI faults 99

## V

- validation 28
- vibration 144
- voltage levels 143
  - separation 143
- voltage-monitoring 143, 144

## W

- watchdog 32, 78



**Fax Transmittal**

**Fax Number: +31 (0)73 6219 125**

**Reader Comments**

To: Honeywell Safety Management Systems, attn. Technical Documentation Group

From:	Name:	Date:	
	Title:		
	Company:		
	Address:		
	City:	State:	Zip:
	Telephone:	Fax:	

Safety Manager Safety Manual, Release 100.3, 25 January 2005

Comments:

---

---

---

---

---

---

---

---

---

---

---

---

You may also call the Technical Documentation Group at +31 (0)73 6273 273,  
email Honeywell SMS at [sms-info@honeywell.com](mailto:sms-info@honeywell.com), or write to:

Honeywell Industry Solutions  
Safety Management Systems  
P.O. box 116  
5201 AC 's-Hertogenbosch  
The Netherlands

**Safety Manager  
User documentation**

# Honeywell

---

Honeywell Industry Solutions  
Safety Management Systems  
Rietveldenweg 32  
5222 AR 's-Hertogenbosch  
The Netherlands